UNITED STATES
NUCLEAR REGULATORY COMMISSION
ADVISORY COMMITTEE ON REACTOR SAFEGUARDS
WASHINGTON, DC 20555 - 0001

June 3, 2004

MEMORANDUM TO: ACRS Members

FROM: Marvin D. Sykes, Senior Staff Engineer
Technical Support Staff
ACRS/ACNW

SUBJECT: CERTIFICATION OF THE MINUTES OF THE ACRS PLANT OPERATIONS SUBCOMMITTEE MEETING ON DIGITAL INSTRUMENTATION AND CONTROL ON MARCH 26, 2004 AT ROCKVILLE, MARYLAND

The minutes of the subject meeting, issued on June 1, 2004 have been certified as the official record of the proceedings of that meeting. A copy of the certified minutes is attached.

Attachment: As stated

cc: J. Larkins
H. Larson
S. Duraiswamy
ACRS Staff Engineers

UNITED STATES
NUCLEAR REGULATORY COMMISSION
ADVISORY COMMITTEE ON REACTOR SAFEGUARDS
WASHINGTON, DC 20555 - 0001

MEMORANDUM TO: Marvin D. Sykes, Senior Staff Engineer, ACRS

FROM: John D. Sieber, Chairman
Plant Operations Subcommittee

SUBJECT: CERTIFICATION OF THE SUMMARY MINUTES OF THE MEETING OF THE ACRS SUBCOMMITTEE ON DIGITAL INSTRUMENTATION AND CONTROL, MARCH 26, 2004 - ROCKVILLE, MARYLAND

I hereby certify, to the best of my knowledge and belief, that the minutes of the subject meeting on March 26, 2004, are an accurate record of the proceedings for that meeting.

June 3, 2004

John D. Sieber, Date
Plant Operations Subcommittee Chairman

UNITED STATES
NUCLEAR REGULATORY COMMISSION
ADVISORY COMMITTEE ON REACTOR SAFEGUARDS
WASHINGTON, DC 20555 - 0001

June 1, 2004

MEMORANDUM TO: John D. Sieber, Chairman
Plant Operations Subcommittee

FROM: Marvin D. Sykes, Senior Staff Engineer, ACRS

SUBJECT: WORKING COPY OF THE MINUTES OF THE ACRS PLANT OPERATIONS SUBCOMMITTEE MEETING ON DIGITAL INSTRUMENTATION AND CONTROL, MARCH 26, 2004 - ROCKVILLE, MARYLAND

A working copy of the minutes for the subject meeting is attached for your review. Please review and comment on them at your earliest convenience. If you are satisfied with these minutes please sign, date, and return the attached certification letter in the pre-addressed envelope attached.

Attachment: Minutes (DRAFT)

cc w/o Attachment:
J. Larkins
H. Larson
S. Duraiswamy
ACRS File

CERTIFIED
6/03/04
By John D. Sieber
Issued: 6/01/04

ADVISORY COMMITTEE ON REACTOR SAFEGUARDS
MINUTES OF ACRS PLANT OPERATIONS SUBCOMMITTEE MEETING
RELATED TO DIGITAL INSTRUMENTATION AND CONTROL
MARCH 26, 2004
ROCKVILLE, MARYLAND

On March 26, 2004, the ACRS Plant Operations Subcommittee held a meeting in Room T-2B3, 11545 Rockville Pike, Rockville, Maryland. The purpose of the meeting was to discuss Office of Nuclear Regulatory Research activities related to digital instrumentation and control (I&C) system reliability modeling.

The meeting was open to the public. No written comments or requests to make oral statements were received from members of the public related to this meeting. Mr. Marvin Sykes was the Designated Federal Official for this meeting. The meeting was convened at 8:30 a.m. and adjourned at 3:55 p.m. on March 26, 2004.

ATTENDEES:

ACRS MEMBERS/CONSULTANTS/STAFF

Jack Sieber, Chairman
Mario Bonaca, Member
Peter Ford, Member
Sergio Guarro, ACRS Consultant
Marvin Sykes, ACRS Staff
George Apostolakis, Member
Tom Kress, Member
Stephen Rosen, Member
James White, ACRS Consultant

ATTENDEES

Steven Arndt, RES
Jiang Hong, NRR
Roman Shaffer, RES
Doug Tifft, RES
Michelle Evans, RES
Carol Smidts, Univ. of Maryland
Jerry Mauck, Framatone ANP
Thomas Roberts, Dept. of Energy
Michael Mayfield, RES
Mike Waterman, NRR
Dean Overland, RES
Tekia Govan, RES
Barry Johnson, Univ. of Virginia
Tsong - Lun Chu, BNL
Ming Li, Univ. of Maryland
Peter Wilson, RES

The presentation slides and handouts used during the meeting and a complete list of attendees is attached to the Office Copy of these Minutes. The presentation to the Subcommittee is summarized below.

Opening Remarks (Subcommittee Chair)
Mr. Jack Sieber, Chairman of the Subcommittee on Plant Operations convened the meeting by providing introductory remarks and later introducing Mr. Michael Mayfield of the Office of Nuclear Regulatory Research (RES) to begin the staff presentation.

Staff Introduction
Michael Mayfield provided brief opening remarks on behalf of the RES staff and introduced Steven Arndt to begin the discussion.

Digital I&C Research Program, State-of-the-Art in Digital System Reliability, Modeling, and PRA Modeling Program
Mr. Arndt began the presentation by providing an overview of the Digital I&C Research Program Plan, discussed in SECY-01-0155. According to Mr. Arndt, the plan addressed several recommendations highlighted in the National Academy of Science (NAS) review. He noted that the goal of the plan was to develop methods for reviewing digital system reliability models to improve the staff's analytical capabilities, and fundamental knowledge of digital technology as demonstrated by the development of analytical tools and techniques. These tools may be used for estimating digital system failure probabilities and for analyzing digital system reliability models. The use of such models is expected to increase overall confidence and reduce uncertainty.

Mr. Arndt explained that the staff has allocated funds for five general research projects for evaluating software reliability. Four of the five projects involved contractual agreements with the University of Virginia (UVa), University of Maryland UMd), Halden Project, and Brookhaven National Laboratories. The fifth projects is an in-house RES effort aimed at developing a working database of reliability information that may assist the staff in the review and validation of licensee assumptions used to justify plant design changes and license amendment requests. It is anticipated that the products of these research studies will assist in improving the NRC's understanding of digital system failure mechanisms and the strengths and limitations of the available digital system modeling techniques.

Mr. Arndt introduced Barry Johnson, UVa and Carol Smidts, UMd to provide more detailed information on their respective research activities.

Digital Systems Modeling Using Fault Injection Methods (UVa)
Mr. Barry Johnson, Director of the Uva Center for Safety-Critical Systems discussed the integrated digital system modeling project to develop a safety assessment process for digital systems. The process uses commercial-of-the-shelf (COTS) hardware and software and fault injection techniques to evaluate reliability. The trial results are statistically correlated to produce measures of software reliability that may be used to assess the reliability and fault tolerance of the integrated digital systems. This approach and the tools that support this approach have been used extensively to assess digital railway control systems and according to Mr. Johnson, the process has already been successfully applied to several other commercial applications. Modeling of the Calvert Cliffs Digital Feedwater Control System is ongoing.

Mr. Johnson also noted that this research project is expected to provide an assessment method that can be used by the NRC staff to independently assess digital system safety and provide additional information on digital system failure modes and reliability that will inform the review process and guidance. The latest application of this assessment method and the input for the associated risk-informed review guidance will be completed in FY 2005.

Metrics Development and Software Reliability Modeling (UMd)
Professor Carol Smidts, UMd discussed the ongoing software metrics project to develop and pilot a systematic framework that can be used by the NRC staff to independently assess and predict software quality and reliability. This assessment tool uses software metrics to predict software quality and reliability under varying operational conditions. The metrics cover the four

aspects of software development, which include requirements specifications, software design, software implementation (coding), and software testing. The quantitative results from this study may be used by the NRC to inform the current review guidance and improve the understanding of software quality and reliability. Large-scale demonstration of this tool in a high reliability nuclear application is planned for completion in early FY 2006.

BNL Research Activities
Steve Arndt briefly discussed the BNL research efforts. BNL is currently engaged in the development of a processor level Markov model for one of the three currently approved platforms to identify the supporting analysis and data needed to model digital design features; development of quantitative methods for assessing software reliability; and digital failure database review.

According to Mr. Arndt , the staff expects to contract with BNL in the future to generate suggestions for improving the integration of digital system risk models into existing PRAs and to develop quantitative methods for reviewing safety-critical systems in PRA-based submittals.

Halden Project
Mr. Arndt explained that the staff is also involved in ongoing work at Halden which includes analysis of operational data related to COTS digital systems, the risk assessment of man-machine interfaces, and the development of tools to assist in combining qualitative and quantitative information in reviews.

Future Plans for Digital System Reliability Modeling
Mr. Arndt provided additional information on future RES plans for continuing and new research projects that will investigate different aspects of risk analysis of digital systems and continually review current and evolving methods. He noted that coordination within the program and with other digital system research in the nuclear and non-nuclear fields is critical.

He restated the scope of the ongoing research activities at UVA, UMd, and BNL and some future proposals. Specifically, he mentioned the proposed research aimed at developing detailed PRA models of sample digital systems, determining the most effective method for digital system modeling, and developing NRC review guidance.

Mr. Arndt closed the presentation by providing information on the expected completion dates for some of the ongoing research studies.

UMd	Early FY 2006 - Intermediate results are to be published in FY 2004.
UVa	FY 2005 - Intermediate results are available.
BNL	FY 2005 - Results of the integration of pilot models into current plant PRAs.

Committee Comments
In general, the Subcommittee recognized that the staff was making considerable progress in developing tools for the evaluation of digital systems that may be used in existing and future plants.

Dr. Apostolakis expressed concern that the RES program may not be on the right path and pondered whether the staff is focusing their efforts on research activities that are most important to the agency. He questioned the staff assertions that the current analysis methods

are sufficiently mature because they have been successfully used in other industries. He also critiqued the staff's review of available reliability models to identify strengths and weaknesses of each prior to selecting Markov modeling for the BNL research.

Mr. Rosen questioned the staff approach to evaluating reliability and development of review guidance. He stressed that the NRC staff should develop detailed guidance and acceptance criteria that clearly delineates what must be included in applications related to digital system reliability. The guidance should also indicate how the applications will be evaluated by the staff. This will alleviate the concerns that he staff has regarding what the applications will look like.

Dr. Kress applauded the bold and proactive efforts that RES has undertaken and thought that the program was well-conceived, and the various parts fit together nicely. Dr. Kress urged continued use of international expertise in this area and suggested that the industry, through EPRI or NEI, get more active in this area. For the UMd study, he suggested that the researchers may need to do more to evaluate the metric data dispersion and factor that into the reliability rankings. The rankings should also be updated as more information is accumulated.

Dr. White agreed that the RES program contents were generally in alignment with recommendations made by the National Academy of Science panel and that the program should provide help in answering the questions expected to be asked about how the NRC will do an assessment. He also noted that it was not apparent whether there were enough such programs to allow the development of comprehensive guidance. He supported the idea of mining Licensee Event Reports to get an idea of the frequency and the mode of digital system failures in existing nuclear plants.

Dr. Guarro noted that the approach taken by the UMd software metrics program was reasonable and the expected results could be used to generate quantitative evaluations of software that could eventually be used in PRA quantification. However, he expressed a belief that there are limitations to the validity of the results. He stated that it was unclear if the "reliability predictive model" and associated ranking for each of the metrics considered would remain confirmed for software with different types of functions and/or programming language.

For the studies conducted at BNL, Dr. Guarro suggested that the staff may need to develop a more in-depth, direct understanding of what the existing analytical methods are good for, or not good for. One way of achieving this may be the performance of benchmark analyses with various methods and for a range of possible use objectives. One may in fact argue that more attention should be given to processes and methods that support multiple uses related to risk assessment, e.g., identifying effective software testing strategies, identifying system / software interface failure modes, enabling bounding quantification for PRA use, etc.

Staff Commitments

During the meeting subcommittee members requested copies of several documents. Some were available while others were in the developmental stages. The staff committed to provide copies of each of the following documents:

1. NUREG/CR-6734, Digital Systems Software Requirements Guideline, Vol. 2

2. EPRI Defense-in Depth and Diversity Topical Report, January 2004 [DRAFT]

3. Brookhaven National Laboratories - Report on the Review of Current Methods and Tools for Modeling Digital Systems, Expected April 2004

4. Brookhaven National Laboratories Review Guidance for Risk-Informed Digital Submittals, Expected Summer 2004

Subcommittee Decisions and Follow-up Actions

The Subcommittee Chairman will make a report to the full Committee during the April 2004 meeting. The Chairman's report will summarize the discussions and make recommendations regarding the need for future discussions on this matter.

Background Materials Provided to the Committee

1. License Renewal Application for the R. E. Ginna Nuclear Power Plant, dated July 30, 2002.

2. Safety Evaluation Report with Open Items Related to the License Renewal of the R. E. Ginna Nuclear Power Plant, October 2003.

2. NRC Inspection Report 50-244/03-010, Scoping and Screening Methodology, dated August 22, 2003.

3. NRC Audit of the R. E. Ginna Nuclear Power Plant Aging Management Programs, dated September 8, 2003.

****

NOTE:
Additional details of this meeting can be obtained from a transcript of this meeting available in the NRC Public Document Room, One White Flint North, 11555 Rockville Pike, Rockville, MD, (301) 415-7000, downloading or view on the Internet at http://www.nrc.gov/reading-rm/doc-collections/acrs/ can be purchased from Neal R. Gross and Co., 1323 Rhode Island Avenue, NW, Washington, D.C. 20005, (202) 234-4433 (voice), (202) 387-7330 (fax), nrgross@nealgross.com (e-mail).

****

Wisconsin. The acceptability of the tendered application for docketing, and other matters including an opportunity to request a hearing, will be the subject of subsequent **Federal Register** notices.

Copies of the application are available for public inspection at the Commission's Public Document Room (PDR), located at One White Flint North, 11555 Rockville Pike (first floor), Rockville, Maryland, 20582 or electronically from the NRC's Agencywide Documents Access and Management System (ADAMS) Public Electronic Reading Room under accession number ML040580020. The ADAMS Public Electronic Reading Room is accessible from the NRC Web site at *http://www.nrc.gov/reading-rm/adams.html*. In addition, the application is available on the NRC Web page at *http://www.nrc.gov/reactors/operating/licensing/renewal/applications.html*, while the application is under review. Persons who do not have access to ADAMS or who encounter problems in accessing the documents located in ADAMS should contact the NRC's PDR Reference staff at 1–800–397–4209, extension 301–415–4737, or by e-mail to *pdr@nrc.gov*.

A copy of the license renewal application for the Point Beach Nuclear Plant, Units 1 and 2, is also available to local residents near the Point Beach Nuclear Plant at the Lester Public Library 1001 Adams Street, Two Rivers, Wisconsin 54241.

Dated at Rockville, Maryland, this 2nd day of March 2004.

For the Nuclear Regulatory Commission.

Pao-Tsin Kuo,

Program Director, License Renewal and Environmental Impacts, Division of Regulatory Improvement Programs, Office of Nuclear Reactor Regulation.

[FR Doc. E4–478 Filed 3–5–04; 8:45 am]

BILLING CODE 7590–01–P

NUCLEAR REGULATORY COMMISSION

Advisory Committee on Reactor Safeguards; Meeting of the Subcommittee on Plant Operations; Notice of Meeting

The ACRS Subcommittee on Plant Operations will hold a meeting on March 26, 2004, Room T–2B3, 11545 Rockville Pike, Rockville, Maryland.

The entire meeting will be open to public attendance.

The agenda for the subject meeting shall be as follows:

Friday, March 26, 2004—8 a.m. Until the Conclusion of Business

The purpose of this meeting is to discuss digital instrumentation and control research activities, including development of digital system reliability models. The Subcommittee will hear presentations by and hold discussions with representatives of the Office of Nuclear Regulatory Research, and other interested persons regarding this matter. The Subcommittee will gather information, analyze relevant issues and facts, and formulate proposed positions and actions, as appropriate, for deliberation by the full Committee.

Members of the public desiring to provide oral statements and/or written comments should notify the Designated Federal Official, Mr. Marvin D. Sykes (telephone 301/415–8716), five days prior to the meeting, if possible, so that appropriate arrangements can be made. Electronic recordings will be permitted.

Further information regarding this meeting can be obtained by contacting the Designated Federal Official between 7:30 a.m. and 4:15 p.m. (e.t.). Persons planning to attend this meeting are urged to contact the above named individual at least two working days prior to the meeting to be advised of any potential changes to the agenda.

Dated: March 1, 2004.

Howard J. Larson,

Acting Associate Director for Technical Support, ACRS/ACNW.

[FR Doc. 04–5104 Filed 3–5–04; 8:45 am]

BILLING CODE 7590–01–P

NUCLEAR REGULATORY COMMISSION

Advisory Committee on Reactor Safeguards: Joint Meeting of the ACRS Subcommittees on Reliability and Probabilistic Risk Assessment and on Plant Operations; Notice of Meeting

The ACRS Subcommittees on Reliability and Probabilistic Risk Assessment and on Plant Operations will hold a joint meeting on March 25, 2004, Room T–2B1, 11545 Rockville Pike, Rockville, Maryland.

The entire meeting will be open to public attendance.

The agenda for the subject meeting shall be as follows:

Thursday, March 25, 2004—8:30 a.m. Until 11:30 a.m.

The Subcommittees will hear the status of the Risk Management Technical Specifications program related to Issue 4(b)—Use of configuration management for determining technical specification completion times. The Subcommittees will hear presentations by and hold discussions with representatives of the NRC staff and other interested persons regarding this matter. The Subcommittees will gather information, analyze relevant issues and facts, and formulate proposed positions and actions, as appropriate, for deliberation by the full Committee.

Members of the public desiring to provide oral statements and/or written comments should notify the Designated Federal Official, Ms. Maggalean Weston (telephone: 301–415–3151) five days prior to the meeting, if possible, so that appropriate arrangements can be made. Electronic recordings will be permitted.

Further information regarding this meeting can be obtained by contacting the Designated Federal Official between 8 a.m. and 5:30 p.m. (e.t.). Persons planning to attend this meeting are urged to contact the above named individual at least two working days prior to the meeting to be advised of any potential changes to the agenda.

Dated: March 2, 2004.

Howard J. Larson,

Acting Associate Director for Technical Support, ACRS/ACNW.

[FR Doc. 04–5105 Filed 3–5–04; 8:45 am]

BILLING CODE 7590–01–P

SECURITIES AND EXCHANGE COMMISSION

[Release No. IC–26373; 812–12817]

Money Market Obligations Trust, et al.; Notice of Application

March 2, 2004.

AGENCY: Securities and Exchange Commission ("Commission").

ACTION: Notice of an application under section 17(b) of the Investment Company Act of 1940 (the "Act") for an exemption from section 17(a) of the Act.

SUMMARY OF APPLICATION: Applicants seek an order under section 17(b) of the act in connection with the transfer of certain assets of Tax-Free Instruments Trust ("TFIT"), a series of Money Market Obligations Trust (the "Trust"), to Edward Jones Tax Free Money Market Fund (the "Jones Fund") in exchange for shares of the Jones Fund.

APPLICANTS: The Trust and the Jones Fund.

FILING DATES: The application was filed on May 1, 2002 and amended on March 1, 2004.

HEARING OR NOTIFICATION OF HEARING: An order granting the application will be issued unless the Commission orders a

ADVISORY COMMITTEE ON REACTOR SAFEGUARDS
PLANT OPERATIONS SUBCOMMITTEE MEETING
DIGITAL INSTRUMENTATION AND CONTROL
MARCH 26, 2004
ROCKVILLE, MARYLAND

- PROPOSED SCHEDULE -

Cognizant Staff Engineer: Marvin D. Sykes MDS1@nrc.gov (301) 415-8716

	TOPICS	PRESENTERS	TIME
I.	**Opening Remarks**	J. Sieber, ACRS G. Apostolakis, ACRS	8:30 -8:35 a.m. 5 minutes
II.	**General Overview of Digital I&C Research Program and Discussion of the State-of-the-Art in Digital System Reliability**	S. Arndt, RES N. Siu, RES	8:35 -9:30 a.m. 55 minutes
III.	**Digital Systems Modeling Using Fault Injection Methods**	B. Johnson, UVa S. Arndt, RES J. Calvert, RES	9:30 -10:15 a.m. 45 minutes
	BREAK		**10:15-10:30a.m.**
III.	**Digital Systems Modeling Using Fault Injection Methods (Continued)**	B. Johnson, UVa S. Arndt, RES J. Calvert, RES	10:30 -11:15 a.m. 45 minutes
IV.	**Static PRA Modeling Program**	S. Arndt, RES D. Overland, RES	11:15 -12:15pm 60 minutes
	LUNCH		**12:15-1:15 p.m.**
V.	**Software Reliability Modeling**	C. Smidts, UMd S. Arndt, RES	1:15-2:30 p.m. 75 minutes
V.	**Staff Plans for Digital Reliability Models**	S. Arndt, RES	2:30-2:50 p.m. 20 minutes
VI.	**General Discussion and Adjourn**	G. Apostolakis, ACRS J. Sieber, ACRS	2:50-3:00 p.m. 10 minutes

NOTE:

- Presentation time should not exceed 50 percent of the total time allocated for a specific item. The remaining 50 percent of the time is reserved for discussion.
- 35 copies of the presentation materials to be provided to the Subcommittee.

ADVISORY COMMITTEE ON REACTOR SAFEGUARDS

SUBCOMMITTEE MEETING PLANT OPERATIONS

March 26, 2004

Date

NRC STAFF SIGN IN FOR ACRS MEETING

PLEASE PRINT

NAME	NRC ORGANIZATION
Peter R Wilson	RES
JIANG HONG	NRR EEIB
Mike Waterman	NRR
Roman Shaffer	RES
Dean Overland	RES
Doug Tifft	RES
STEVEN ARNOT	RES
Tekia [illegible]	RES
Michele Evans	RES

ADVISORY COMMITTEE ON REACTOR SAFEGUARDS

SUBCOMMITTEE MEETING ON PLANT OPERATIONS

March 26, 2004
Date

v

PLEASE PRINT

NAME	AFFILIATION
Barry W. Johnson	University of Virginia
TSONG-LUN CHU	BROOKHAVEN NATIONAL LAB.
Carol Smidts	University of Maryland.
~~JIANG HONG~~	
Jerry Mauck	Framatome ANP
Ming Li	Univ. of Maryland
Thomas E. Roberts	DOE (Naval Reactors)

Software Reliability Modeling

The Use of Software Measures to Predict Software Quality and Reliability

PRESENTED BY

Prof. Carol Smidts

csmidts@eng.umd.edu

COAUTHORED BY

Dr. Ming Li

mli@wam.umd.edu

March 26, 2004

Conclusions

- A method to use software measures as a quantitative technique for predicting software quality and reliability has been developed and piloted
- The results of this method to date have been very promising.
- The method parallels the current review method, so it should be straight forward to implement
- Work is currently ongoing to validate the method on a large, high reliability nuclear application.

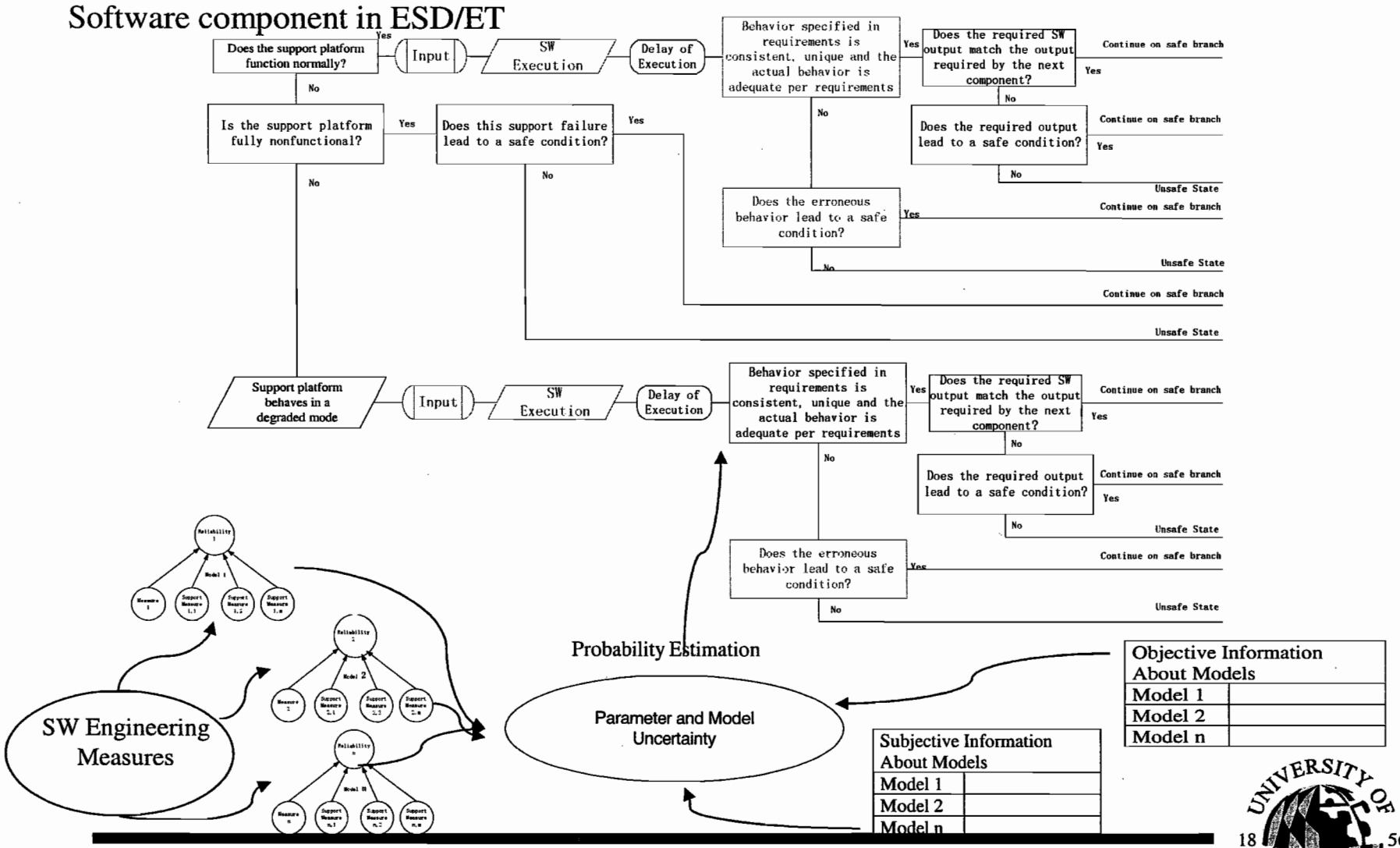
The primary objective of this research is to provide a systematic framework to enhance current review practice for software in the NRC.

Project History

- Lawrence Livermore National Laboratory (LLNL) Study (1996 –1998)
- University of Maryland
  - Expert Opinion Study (1998 – 2000)
  - Validation Study (2001 – 2002 (9 months))
  - Large-Scale Validation Study (2004 - present)

PRA Framework for I&C Systems

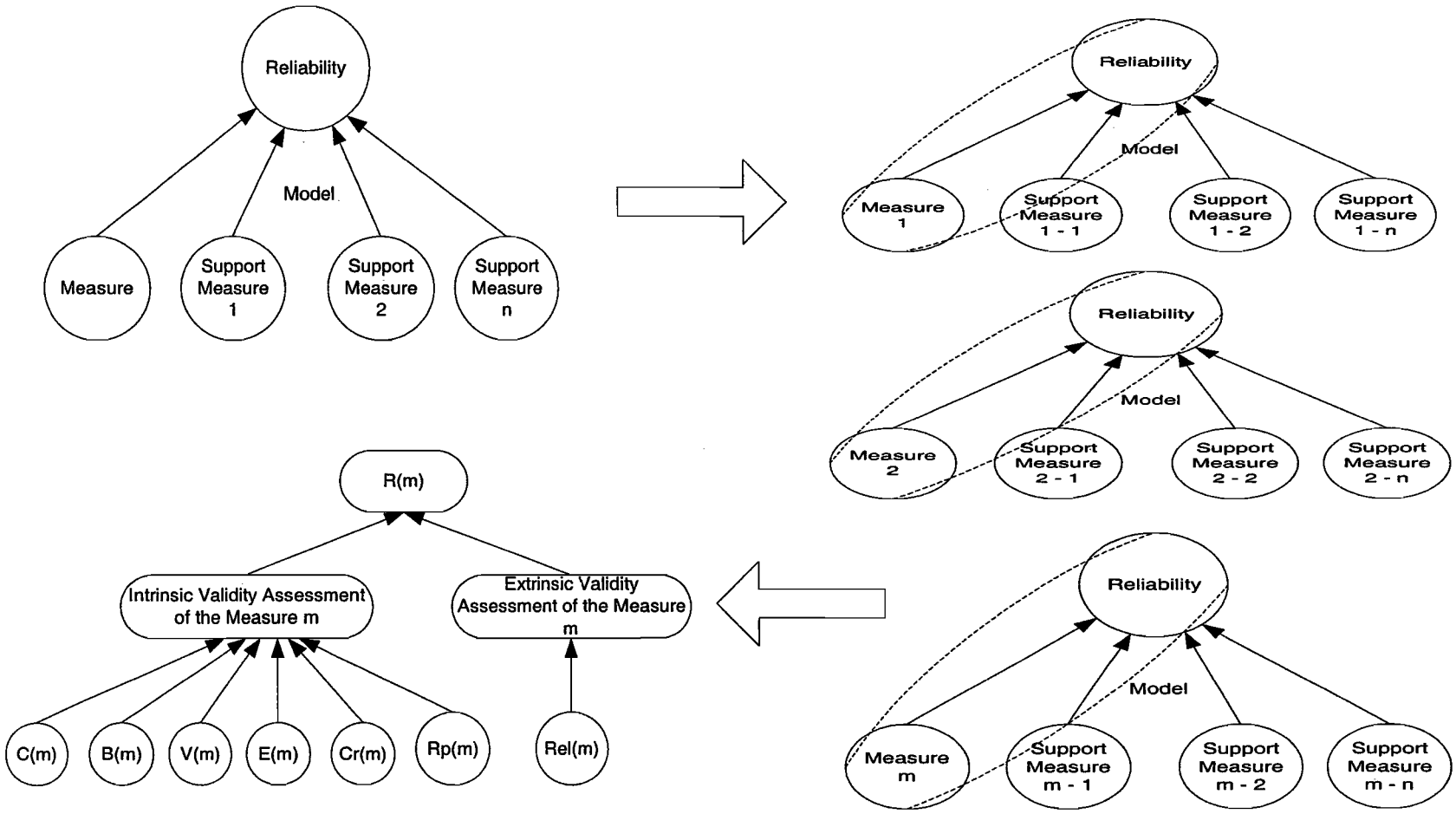
Software component in ESD/ET



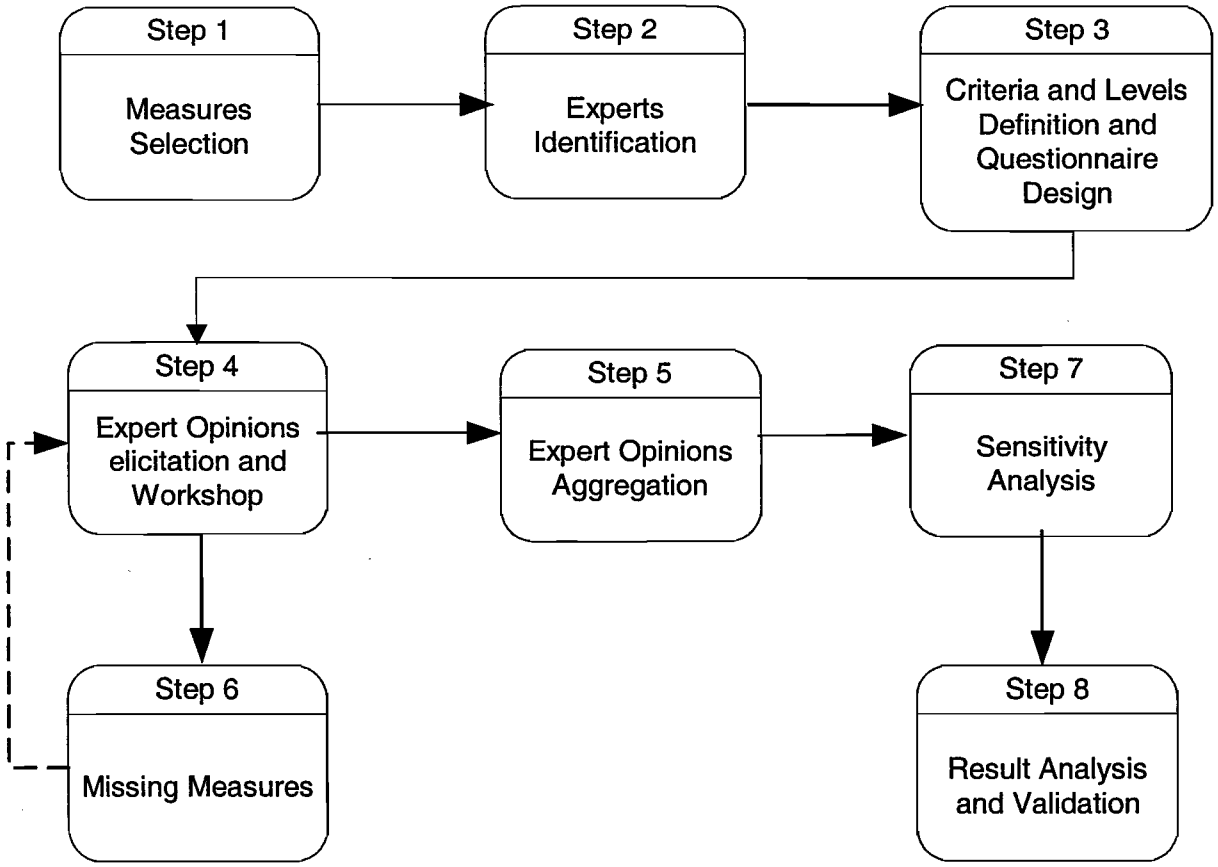
Philosophy Behind This Research

- How is software reliability determined?
  - Product characteristics
    - Project characteristics
    - Development characteristics
  - Operational environment
- Software engineering measures determine software reliability

From Measures to Reliability



Ranking Process



Experts Selection

Expert	Occupation	Area of Expertise
Alain Abran	Industry/Academia	Telecommunication, Financial
David Card	Industry	Software measurement and process improvement
William Everett	Industry	Telecommunication, Aerospace
Jon Hagar	Industry	Aerospace
Herbert Hecht	Industry	Nuclear, Aerospace
Watts Humphrey	Industry/Academia	Aerospace
Michael Lyu	Industry/Academia	Telecommunication, Aerospace
Jean-Claude Laprie	Academia	Telecommunication, Aerospace
William Petrick	Industry	Nuclear
Allen Nikora	Academia	Software reliability modeling

Pre-selected 30 Measures

- Intermediate Results from LLNL:

Bugs per line of code (Gaffney estimate)
Cause & effect graphing
Code defect density
Cohesion
Completeness
Cumulative failure profile
Cyclomatic complexity
Data flow complexity
Design defect density
Error distribution
Failure rate
Fault density
Fault number days
Feature point analysis
Function point analysis
Functional test coverage
Graph-theoretic static architecture complexity
Man hours per major defect detected
Mean time to failure
Minimal unit test case determination
Modular test coverage
Mutation testing (error seeding)
Number of faults remaining (error seeding)
Requirements compliance
Requirements specification change requests
Requirements traceability
Reviews, inspections and walkthroughs
Software capability maturity model
System design complexity
Test coverage

Ranking Results

Measure	Development Phase			
	Requirements	Design	Implementation	Testing
Bugs per line of code (Gaffney estimate)			0.44	0.37
Cause & effect graphing	0.45	0.43	0.40	0.45
Code defect density			0.83	0.83
Cohesion		0.45	0.37	0.37
Completeness	0.41	0.33	0.33	0.33
Cumulative failure profile				0.80
Cyclomatic complexity		0.74	0.77	0.74
Data flow complexity		0.63	0.60	0.60
Design defect density		0.77	0.77	0.76
Error distribution	0.70	0.70	0.69	0.69
Failure rate				0.87
Fault density	0.73	0.76	0.77	0.77
Fault number days	0.63	0.73	0.73	0.75
Feature point analysis	0.44	0.47	0.47	0.43
Function point analysis	0.51	0.54	0.55	0.50
Functional test coverage				0.61
Graph-theoretic static architecture complexity		0.52	0.45	0.45
Man hours per major defect detected		0.65	0.63	0.65
Mean time to failure				0.81
Minimal unit test case determination			0.65	0.71
Modular test coverage				0.70
Mutation testing (error seeding)				0.47
Number of faults remaining (error seeding)	0.45	0.45	0.47	0.50
Requirements compliance	0.52	0.50	0.51	0.50
Requirements specification change requests	0.71	0.71	0.71	0.70
Requirements traceability		0.58	0.57	0.57
Reviews, inspections and walkthroughs	0.62	0.61	0.61	0.62
Software capability maturity model	0.62	0.62	0.61	0.61
System design complexity		0.56	0.55	0.55
Test coverage				0.70

Ranking of Top 5 Non-OO Measures per Phase

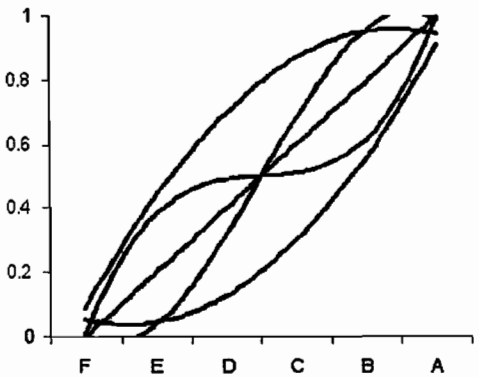
Rank	Requirements	Design	Implementation	Testing
1	Fault density	Design defect density	Code defect density	Failure rate
2	Requirements specification change requests	Cyclomatic complexity	Design defect density	Code defect density
3	Error distribution	Fault density	Cyclomatic complexity	Coverage factor
4	Reviews, inspections and walkthroughs	Fault number days	Fault density	Mean time to failure
5	Fault number days	Requirements specification change requests	Fault number days	Cumulative failure profile

10 Missing Measures

Coverage factor
Full function point (FFP)
Mutation score
Class coupling
Class hierarchy nesting level
Lack of cohesion of methods (LCOM)
Number of children (NOC)
Number of class methods in a class
Number of key classes
Weighted method per class

Sensitivity Analysis - Variations

Letter – Real Conversion



Aggregation Weight

Co	Be	Cr	Rep	Ex	Va	Rel
0.14	0.14	0.14	0.14	0.14	0.14	0.14
0.13	0.13	0.13	0.13	0.13	0.13	0.25
0.08	0.08	0.17	0.17	0.08	0.08	0.33
0.245	0.045	0.088	0.036	0.130	0.239	0.216
0.20	0.03	0.10	0.17	0.16	0.14	0.20
0	0	0.25	0.25	0.25	0	0.25

Aggregation Function

- Additive
- Multiplicative

Ranges of Correlation Coefficients

Correlation Coefficient Range	Rate Count	Ranking Count
0 – 0.8	0	1
0.8 – 0.9	4	8
0.9 - 0.99	90	92
0.99 – 1.0	11	4

Validation Method

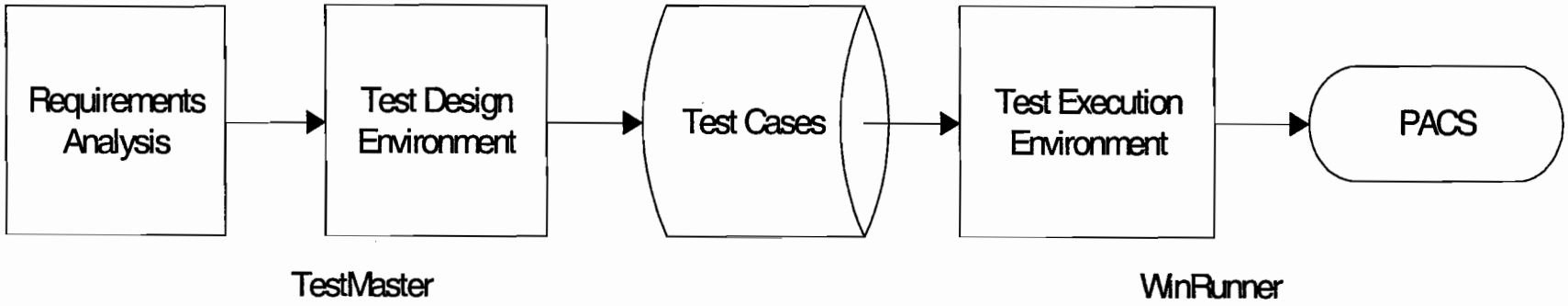
1. Selection of the Application;
2. Measures/Families Selection;
3. Reliability Assessment;
4. Construction of Reliability Prediction Systems;
5. Measurement and Analysis;
6. Peer Review

Validation

- Application under validation: PACS
  - PACS 1: CMM Level 4, Industry developed, C++, reliability ~ 0.92 per demand
  - PACS 2: West Virginia University developed, C++, reliability ~ 0.999 per demand (Sponsored by NASA)
- Measures used in validation:
  - Mean time to failure
  - Defect density
  - Test coverage
  - Requirements traceability
  - Function point
  - Bugs per line of code (Gaffney estimate)

Reliability Assessment

- Reliability testing environment



The Operational Profile

No	Description of the Event	Probability
1.	Entering a good card: A good card is card that has the card data in the correct format and has a data that's in the database. In other words this event reflects the number of times a genuine card is being entered in the system.	0.97
2.	Entering a good PIN: A good PIN is the event that reflects that the four digits of the PIN are correct and match the entry in the database.	0.8
3.	Entry of the 1st digit within time: The allowed time for entry of the first digit of the PIN is 10 seconds.	0.98
4.	Entry of subsequent digits of PIN within time: The allowed time is 5 seconds	0.97
5.	Erasure of a PIN digit: The PIN digits are erased whenever the keys # or * are pressed.	0.001
6.	User able to pass within the stipulated time after opening of gate	0.99
7.	Guard is requested for extra time	0.01
8.	Guard allows extra 10 seconds.	0.01
9.	Guard Override: This event refers to the event of the guard over riding the verdict of the system. The system passes control to the guard after three failed attempts of entry of PIN/ Card. The message "See Officer" is displayed on the LED and the guard has the ability to allow the user to get in (over ride) or reset the system to its initial state.	0.5
10.	Hardware Failure : Although failure of any register from R1 to R11 will induce a system failure, only failure of register R5 and combined failure of registers R1, R2, R3, R4 and R9 results in a failure of level 1. The failure probability is calculated assuming probability of failure of a typical register to be 0.001 per demand.	0.001

Reliability Assessment

- Reliability is determined by:

$$R = \frac{n - r + 1}{n + 1}$$

R	Reliability
n	Number of runs
r	Number of failures

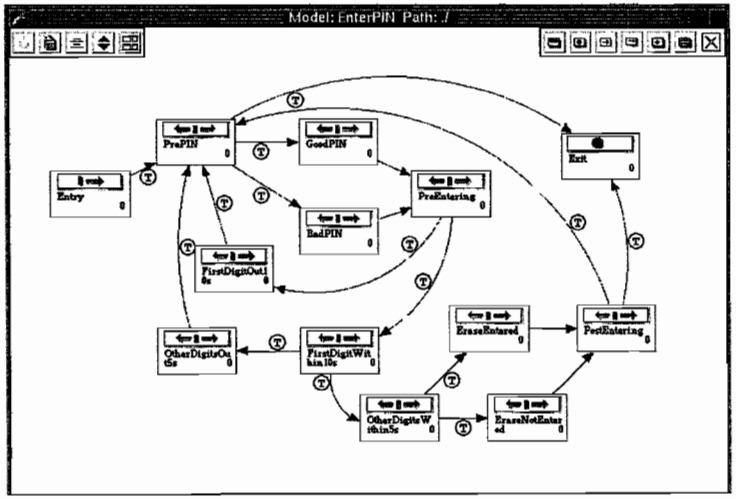
RePSs

- MTTF RePS

$$P_s = e^{-\frac{1}{\rho.MTTF}}$$

- Defect Density RePS

$$p_s = 1 - \oint_i P(i) * I(i) * E(i)$$



RePSs

- Test Coverage RePS
  - Derive the number of defects remaining from the number of defects tested.

$$C^0 = a_0 \ln[1 + a_1 (\exp(a_2 C_1) - 1]$$

$$N = N^0 / C^0$$

$$p_s = e^{-\frac{K}{T_L} N\tau}$$

  - C_1: statement coverage
  - K: fault exposure ratio obtained using the finite state machine model.

RePSs

- Requirements Traceability RePS
  - Each untraceable requirement is a defect
  - Apply the Finite State Machine techniques used in Defect Density RePS to obtain the value of *Ps*
- Function Point Analysis
  - Derived the number of defects remaining from the Function Point counting using Capers Jones data (see next slide)
  - Applying $p_s = e^{-\frac{K}{T_L} N\tau}$
  - *K* is obtained from the literature

Excerpt From the Literature*

Function points	Severity 1 (critical)	Severity 2 (significant)	Severity 3 (minor)	Severity 4 (cosmetic)	Total
1	0	0	0	0	0
10	0	0	1	0	1
100	1	4	14	20	39
1,000	6	78	222	250	556
10,000	127	1,225	4,224	2,872	8,448
100,000	2,658	15,946	66,440	47,837	132,880
Average	465	2,875	11,817	8,497	23,654
Percent	1.97	12.16	49.96	35.92	100.00

* Table 3.48 from Capers Jones, *Applied Software Measurement: Assuring Productivity and Quality,* 2nd Edition, McGraw-Hill, New York, 1996

RePSs

- Bugs per Line of Code
  - Obtain the number of defects remaining from the LOC using an empirical relationship

    $$F = \sum_{i=1}^{N} (4.2 + 0.0015 S_i^{4/3})$$

  - Applying $p_s = e^{-\frac{K}{T_L} F \tau}$
  - K is obtained from the literature

Prediction Quality Indicator: *pe*

- Definition

$$pe = \frac{|\, p_s(real) - p_s(est) \,|}{1 - p_s(real)}$$

pe	Prediction error
$p_s(real)$	The probability of success per demand obtained from reliability testing
$p_s(est)$	The probability of success per demand obtained from the RPS

Validation Results for PACS 1

Measure	Value	p_s^*	*pe*	Original Rankings Based on Expert Opinion	Rankings Based On Validation
Mean time to failure	1267.6 seconds	0.91849	0.0296	1	1
Defect density	11.72 defects/KLOC	0.92243	0.0766	2	2
Test coverage	94.6%	0.90800	0.0952	3	4
Requirements traceability	78.6%	0.92243	0.0766	4	3
Function point	75.0	0.998546	0.9827	5	6
Bugs per line of code (Gaffney estimate)	66 (65.6) defects	0.979902	0.7607	6	5
p_s(real)	0.916				

UNIVERSITY OF MARYLAND 1856

Peer Review for PACS1

- The validation research was reviewed by four internationally known experts
  - David Card
  - Jon Hagar
  - Herbert Hecht
  - Michael Lyu

Validation Results for PACS 2 *

Measure	Value	p_s	pe	Original Rankings Based on Expert Opinion	Rankings Based On Validation
Defect Density	5.60 defects/KLOC	0.9989	0.2667	2	2
Test Coverage	97.2%	0.9988	0.2	3	4
Requirements Traceability	97.0%	0.9989	0.2667	4	3
Function Point	78	0.9977	0.5333	5	5
Bugs per Line of Code	33.4	0.9853	8.8	6	6
The real reliability estimation	0.9985				

* Funded by NASA IV&V

Related Publications

- Li, M., Smidts, C., "A Ranking of Software Engineering Measures Based On Expert Opinion", *IEEE Transactions on Software Engineering*, pp. 811-24, Vol. 29 No. 9, Sept. 2003.
- Smidts C., Li M., "Software Engineering Measures for Predicting Software Reliability in Safety Critical Digital Systems", prepared for the U.S. Nuclear Regulatory Commission, NUREG/GR-0019, UMD-RE-2000-23, U.S. Nuclear Regulatory Commission, Office of Nuclear Regulatory Research (2000).
- Li M., Smidts C., "Ranking Software Engineering Measures Related to Reliability Using Expert Opinion", Proceedings of ISSRE, p. 246 – 258, San Jose, California, 8-11 October, 2000.
- Smidts, C., Cukic, B., et al, "Software Reliability Corroboration", NASA Software Engineering Workshop, Greenbelt, MD, 4-6 December 2002.

Current Research

- Larger application, more measures and full lifecycle
  - Larger application: STAR system
  - More measures: Coverage Factor, CMM, Fault Days Number, Requirements Specification Change Request, Cause and Effect Graphing, Mutation Testing
  - Full lifecycle: requirements, design, coding, testing
- Improvements for RePSs
  - The estimation of the number of unknown defects
  - The PIE characteristics for unknown defects
  - The estimation of the "true" fault exposure ratio

Summary

- A method to use software measures as a quantitative technique for predicting software quality and reliability has been developed and piloted
- The results of this method to date have been very promising.
- The method parallels the current review method, so it should be straight forward to implement
- Work is currently ongoing to validate the method on a large, high reliability nuclear application.

United States Nuclear Regulatory Commission

ADVISORY COMMITTEE ON REACTOR SAFEGUARDS PLANT OPERATIONS SUBCOMMITTEE MEETING ON DIGITAL INSTRUMENTATION AND CONTROL

March 26, 2004

Division of Engineering Technology
Office of Nuclear Regulatory Research

United States Nuclear Regulatory Commission

SCHEDULE

Opening Remarks	8:30-8:35AM
Overview of Digital I&C Research Program, State-of-the-Art in Digital System Reliability, Modeling and PRA Modeling Program	8:35-10:00AM
Break	10:00-10:15AM
Overview of Digital I&C Research Program, State-of-the-Art in Digital System Reliability, Modeling and PRA Modeling Program (Continued)	10:15-10:45AM
Digital Systems Modeling Using Fault Injection Methods	10:45AM-12:15 PM
Lunch	12:15-1:15 PM
Software Reliability Modeling	1:15-2:30 PM
Staff Plans for Digital Reliability Models	2:30-2:50 PM
General Discussion and Adjourn	2:50-3:00 PM

United States Nuclear Regulatory Commission

Overview of Digital I&C Research Program, State-of-the-Art in Digital System Reliability Modeling and PRA Modeling Program

Steven A. Arndt
(saa@nrc.gov, 301-415-6502)
Division of Engineering Technology
Office of Nuclear Regulatory Research

March 26, 2004

OVERVIEW

- Conclusions
- Review of digital I&C research program
- Drivers and boundary conditions
- Digital system reliability modeling
- Current methods
- Research projects
- Summary

CONCLUSIONS

- NRC research program will answer important questions associated with digital system risk analysis
- Research includes model development, data collection and analyses, and guidance development
- Several of the tool development programs are at the demonstration phase
- NRC is working with other researchers to keep abreast of the current state-of-the-art

CONCLUSIONS (CONT)

- Current analysis methods are sufficiently mature such that guidance documents can be developed
- Current state of the practice analysis methods have significant weaknesses
- Future work is needed to develop and test an integrated PRA model to support audit calculations
- Research is needed to develop additional data and better use the data that is available
- Additional coordination within the international community is needed and planned

DIGITAL I&C RESEARCH PROGRAM PLAN

- SECY-01-0155, NRC digital instrumentation and control research plan, published August 2001
- Addressed the need highlighted in the NAS review for a more systematic approach to developing new information and regulatory guidance
- Endorsed by the ACRS and commission
- Includes research in five major areas
- New research plan under development

I&C RESEARCH PROGRAM GOALS

- I&C research program goal
  - "Continually improving the staff's analytical capabilities, and fundamental knowledge of digital I&C technology as demonstrated by the development of analytical tools, technical reports, regulatory guidance, papers and articles, and interaction with licensees, vendors, industry research organizations, and the public."

I&C RESEARCH PROGRAM GOALS (CONT.)

- Examples of I&C research program products
  - New analytical methods, such as the UVa method
  - Updated regulatory guidance, such as RG 1.168 on "Verification, Validation, Reviews and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants"
  - Technical support of other NRC programs
    - MOX and centrifuge for NMSS
    - Flowmeter work for NRR
    - Software quality work for RES and OIG

DIGITAL I&C RESEARCH PROGRAM

- System aspects of digital technology
  - Environmental stressors
  - Digital requirement specifications
  - Diagnostics and fault-tolerance
  - Operating systems

DIGITAL I&C RESEARCH PROGRAM (CONT)

- Software quality assurance
  - Objective software engineering criteria
  - Criteria for software testing

DIGITAL I&C RESEARCH PROGRAM (CONT)

- Emerging I&C technologies and applications
  - Predictive maintenance and on-line monitoring
  - Advanced instrumentation
  - Smart transmitters
  - Wireless communication
  - Computer security
  - Reviewing technologies and infrastructure including developing and maintaining interactions and interfaces, and standards work

DIGITAL I&C RESEARCH PROGRAM (CONT)

- Advanced reactor I&C infrastructure
  - Lessons learned from evolutionary plants
  - Technical and regulatory issues encountered in new reactor construction around the world
  - Development of risk models for advanced plants
  - Other projects in research program but not yet funded include:
    - Review of issues associated with multi-module plants
    - Autonomous control
    - New instruments, and advanced diagnostics

DIGITAL I&C RESEARCH PROGRAM (CONT)

- Risk assessment of digital I&C systems
  - Digital I&C failure data research
  - Digital failure assessment methods and system models
  - Digital reliability assessment methods and integration in PRA's
  - Digital system risk guidance

RESOURCES

- FY 2004 I&C section budget is 9 FTE and $3.8M
  - ~1 FTE and $1.0 M devoted to digital system reliability and risk modeling
  - The remaining resources are devoted to the other parts of the digital I&C research program, system aspects, software quality assurance, emerging I&C technologies and advanced reactor research

PRA PROGRAM EXTERNAL DRIVERS

- NAS recommendations
- DOE I&C and HMI Working Group recommendations, May 2002
- Halden Workshop on Digital System Reliability, December 2002
- DRAFT EPRI D-i-D&D Topical Report, January 2004

DIGITAL SYSTEM PRA RESEARCH

- NAS "Digital Instrumentation and Control Systems in Nuclear Power Plant" Report Recommendations

- NRC PRA Policy

NAS REPORT RECOMMENDATIONS

- Include the relative influence of software failures on system reliability in PRAs
- Develop methods for estimating digital system failure probabilities, including COTS. Include acceptance criteria, guidelines, limitations, rationale and justifications
- Develop advanced techniques for analyzing digital systems to increase confidence and reduce uncertainty in quantitative assessments
- NRC and industry should evaluate their capabilities and develop a sufficient level of expertise to understand the requirements of digital implementations of system functions and the limitations of quantitative assessments

NRC PRA Policy

- Increase the use of PRA in all regulatory matters to the extent supported by state-of-the-art methods and data in a manner that complements a deterministic approach and supports the traditional defense-in-depth philosophy

WHAT IS NEEDED IN DIGITAL SYSTEM PRAs

- Develop methods for reviewing digital system reliability models
  - Understanding the state of the data
  - Digital system failure mechanisms
  - Strengths and limitations of digital system models
  - Incorporating digital system models into PRAs
  - Acceptability criteria

RESEARCH PRODUCTS

- Improve the review process by providing additional information, guidance and tools
- To accomplish this RES needs to:
  - Develop a detailed understanding of the technology
  - Provide guidance that will improve the review process by making it more
    - Quantitative
    - Realistic
    - Repeatable
  - Develop tools that can be used to assist the reviews, inform reviews or be used to perform check calculations

RESEARCH PRODUCTS

- For the risk assessment projects this tool box will include:
  - NUREGs that will provide information on how digital systems fail and the strengths and limitations of digital system models
  - Guidance that will permit more quantitative reviews
    - Guidance on acceptability of risk informed digital submittals
    - Guidance on quantitative measures of software quality and reliability
    - Guidance on alternate methods for demonstrating system safety
  - Data and analysis to inform reviews and validate assumptions
  - Check tools to independently assess digital system submittals

RESEARCH PROJECTS

- UVa Integrated digital system modeling project
- UMd software metrics project
- BNL project on digital system risk
- Other database development
  - COMPSIS
  - NRC In-house effort
- Other efforts
  - Halden
  - CSNI initiative

STRUCTURE OF CURRENT NRC RESEARCH

- UVa integrated digital system modeling project will provide:
  - An integrated digital system assessment method that can be used by the NRC staff to independently assess digital system safety
  - Information on digital system failure modes and reliability that will inform the review guidance

STRUCTURE OF CURRENT NRC RESEARCH (CONT)

- UMd software metrics project will provide:
  - An assessment method that can be used by the NRC staff to independently assess software quality and reliability
  - Quantitative information on the relative importance of software metrics will be used to inform the current review guidance
  - Input to guidance on quantitative software quality and reliability

STRUCTURE OF CURRENT NRC RESEARCH (CONT)

- BNL project on digital system risk will provide:
  - Draft interim review guidance for risk informed digital submittals
  - Review current methods and tools for modeling digital systems that will be used in guidance for risk informed digital submittals
  - Review of digital failure databases
  - Digital system PRA model

STRUCTURE OF CURRENT NRC RESEARCH (CONT)

- Other database development
  - Data and analysis to inform reviews and validate assumptions
- Halden
  - Analysis of operational data to support risk analysis of COTS systems
  - Risk assessment of human system interfaces
  - A tool to assist in combining qualitative and quantitative information in reviews

DIGITAL SYSTEM RELIABILITY MODELING

- Modeling issues
  - Models should include important failure modes
  - Level of detail of the models
  - Independence of hardware and software
  - Software diversity
  - Number of possible states and the ability to test
- Modeling requirements
  - Ability to predict
  - Supported by or at least consistent with data

DIGITAL SYSTEM RELIABILITY MODELING (CONT)

- Various analysis methods have been proposed
  - Fault trees
  - Markov analysis
  - Dynamic flow graph methodology
  - Petri nets
- Setting acceptance criteria for both the modeling fidelity and the system reliability will be difficult

CURRENT METHODS

- In the nuclear industry, use of these methods is limited
- Most methods in trial use today focus on independent software modeling using software fault trees or other similar methods
- Some methods use "bounding" methods to assume digital system reliability
- Most methods in current use assume that the software can be analyzed separate from its hardware context
- The NRC will need to be able to review what is submitted

OBJECTIVES OF THE BNL PROJECT ON DIGITAL SYSTEM RISKS

- Development of guidance for reviewing PRA-based submittals for digital systems
- Investigate strengths and weaknesses of current digital systems analysis methods
- Generate suggestions for improving the integration of the methods with PRA
- Review of digital failure databases

BNL PRODUCTS

- Review current methods and tools for modeling digital systems
- List of issues associated with probabilistic failure modeling of digital systems
- Draft interim review guidance on PRA of digital systems
- FMEA of one of the generically approved digital platforms
- Review of digital failure databases

DRAFT INTERIM REVIEW GUIDANCE ON PRA OF DIGITAL SYSTEMS

- Prepared in anticipation of up-coming industry submittals (not yet received)
  - Identifies information needed for review of PRA models of digital systems
  - Makes use of the information generated by the deterministic evaluation

DRAFT INTERIM REVIEW GUIDANCE ON PRA OF DIGITAL SYSTEMS (CONT)

- Guidance
  - Refers to qualitative assessment of digital upgrade impacts derived from deterministic analyses
    - FMEA
    - Hazard analysis
    - Abnormal conditions and events (ACEs)
    - New initiating events
  - Notes need for modeling of dependencies - communication links, voting, synchronization
  - Refers to quantitative criterion based on RG 1.174

MODELING DIGITAL SYSTEMS ISSUES

- Software failures
  - Probabilistic modeling
  - Methods exist for quantifying digital safety system reliability, however, there is no common agreement among experts as to which methods are best or appropriate
  - Common cause failures

MODELING DIGITAL SYSTEMS ISSUES (CONT)

- Hardware failures
  - What is the level at which component failures should be modeled? What are the failure modes?
  - Does existing failure data adequately capture the unique features of digital systems? What about CCF?
- Software-hardware interactions
- Integration of digital systems models within existing PRAs

REVIEW OF METHODS AND TOOLS FOR MODELING DIGITAL SYSTEMS

- AP600 PRA - Fault Tree Analysis
- Dynamic Flow Methodology
- GO Methodology
- INEL RPS studies - Fault Tree Analysis of Analog Designs
- Petri Net Method - behavior mode, conversion to Markov
- Fault Injection Method - Markov Model

REVIEW OF METHODS AND TOOLS FOR MODELING DIGITAL SYSTEMS (CONT)

- Study of generically approved digital platform reliability/availability - markov Model and FMEA
- International Electrotechnical Commission (IEC) standard 61508
- Bayesian belief network
- EPRI report on applying risk-informed method to defense-in-depth and diversity evaluation

FMEA

- Conducted analysis of a hypothetical RPS based on a generically approved digital platform
- A top down, step-by-step approach focusing on increasing levels of detail
- Identified potential dependencies
- Generated list of questions and issues about design

INSIGHTS FROM FMEA

- In order to capture the benefits of redundancy and address potential adverse dependencies, a detailed probabilistic model must be developed and supported by deterministic evaluations
  - NRC has not endorsed any generic methods for addressing communication between redundant channels
- FMEA of detailed levels requires detailed design information and a simulation model of the design (which were not available)

DATABASE REVIEW

- Review of NRC publications
  - LER searches by NRC staff, NUREG/CR-6734 Vol 2
- Review of publicly available databases
  - 217F
  - PRISM
  - TELCORDIA
- PRISM and TELCORDIA databases
- Other sources of data that can be pursued
  - GIDEP – Reports of government agencies
  - Other industries and government agencies
  - Manufacturers may have additional data

DATABASE REVIEW (CONT)

- Software failures have caused serious accidents in other industries, Therac 25, 1985-1987, Airbus crash,1994, etc.
- NRC LER searches 1994-1998 and NUREG/CR-6734 Vol 2
  - 8% of all LERs contain digital I&C failures
  - 9% of reactor trips can be attributed to digital I&C failures
  - Digital failures are approximately evenly divided among hardware, software, and human system interface related failures

DATA BASE REVIEW (CONT)

- Military Handbook 217F, Telcordia, PRISM
  - Military hand book uses parts count and part stress methods to estimate failure rate of series systems
  - Telcordia and databases of other countries are similar
  - PRISM (Reliability Analysis Center) included more recent failure data, provided guidance on use of process grading factors to account for design and manufacturing variability at system level, and provided guidance on use of CMM, Radio Technical Commission for Aeronautics (RTCA) safety level, and ISO 9000 certification to estimate software MTTF using a reliability growth model.

DATABASE REVIEW (CONT)

- Military Handbook 217F, Telcordia, PRISM
  - Failure rates were estimated by dividing the number of reported failures by the total operating time
  - Redundancy of safety channels must be modeled outside the databases
  - Fault tolerance features are implicit in the failure rate estimates, i.e., if a fault is detected and corrected automatically, no failure is reported
  - Original failure reports are not publicly available

FINDINGS OF BNL REVIEW

- Acceptable quantitative methods for assessing software failure probability are needed
- Markov-type modeling at the processor level appears to be capable of capturing digital design features
- Probabilistic modeling must be supported by detailed deterministic evaluations
- Data is needed to support detailed probabilistic modeling, failure rates, and diagnostic coverage

OTHER DATABASE DEVELOPMENT

- COMPSIS
  - International effort to develop a database of software failures in computer systems important to safety in nuclear plants, and the lessons learned from these failures
- NRC In-House Effort
  - Project to develop an NRC database of digital system failure information for use in validating reliability modeling assumptions

OTHER EFFORTS

- Halden Reactor Project program
  - As part of the CY 2003-2005 program plan, Halden determined that they would greatly expand their work in digital system safety
  - Part of their new work will be in digital system risk assessment
  - This new work includes analysis of operational data to support risk analysis of COTS systems, risk assessment of human system interfaces, and the use of BBNs to combine qualitative and quantitative information

OTHER EFFORTS (CONT)

- The CSNI has expressed interest in expanding its role in digital system safety research
- NRC staff will lead a briefing in June by various member countries
- This may result in an expert group assessing this technology and/or a new working group
- The NRC is also holding discussions about starting an international program in this area

SUMMARY

- Digital system reliability projects include model development, data collection and analysis, and guidance development
- Several tool development projects are in the demonstration phase
- US nuclear industry is moving forward in this area and the NRC research program is working to provide tools, methods, and guidance to support reviews in this area
- Current analysis methods are sufficiently mature such that guidance documents can be developed

SUMMARY (CONT)

- Current methods have significant strengths and weaknesses
- Future work is needed to develop and test an integrated PRA model to support audit calculations
- Research is needed to develop additional data and better use the data that is available
- Additional coordination within the international community is needed and planned

Digital Systems Modeling Using Fault Injection Methods

Presentation to ACRS at NRC

Barry W. Johnson, Ph.D.
(bwj@virginia.edu)
Director, UVA Center for Safety-Critical Systems

March 26, 2004

Presentation Outline

- Conclusions
- Research Objectives
- Background
- Challenges
- System Modeling Methodology
- Safety Assessment Process
- Applications
- Summary

Conclusions

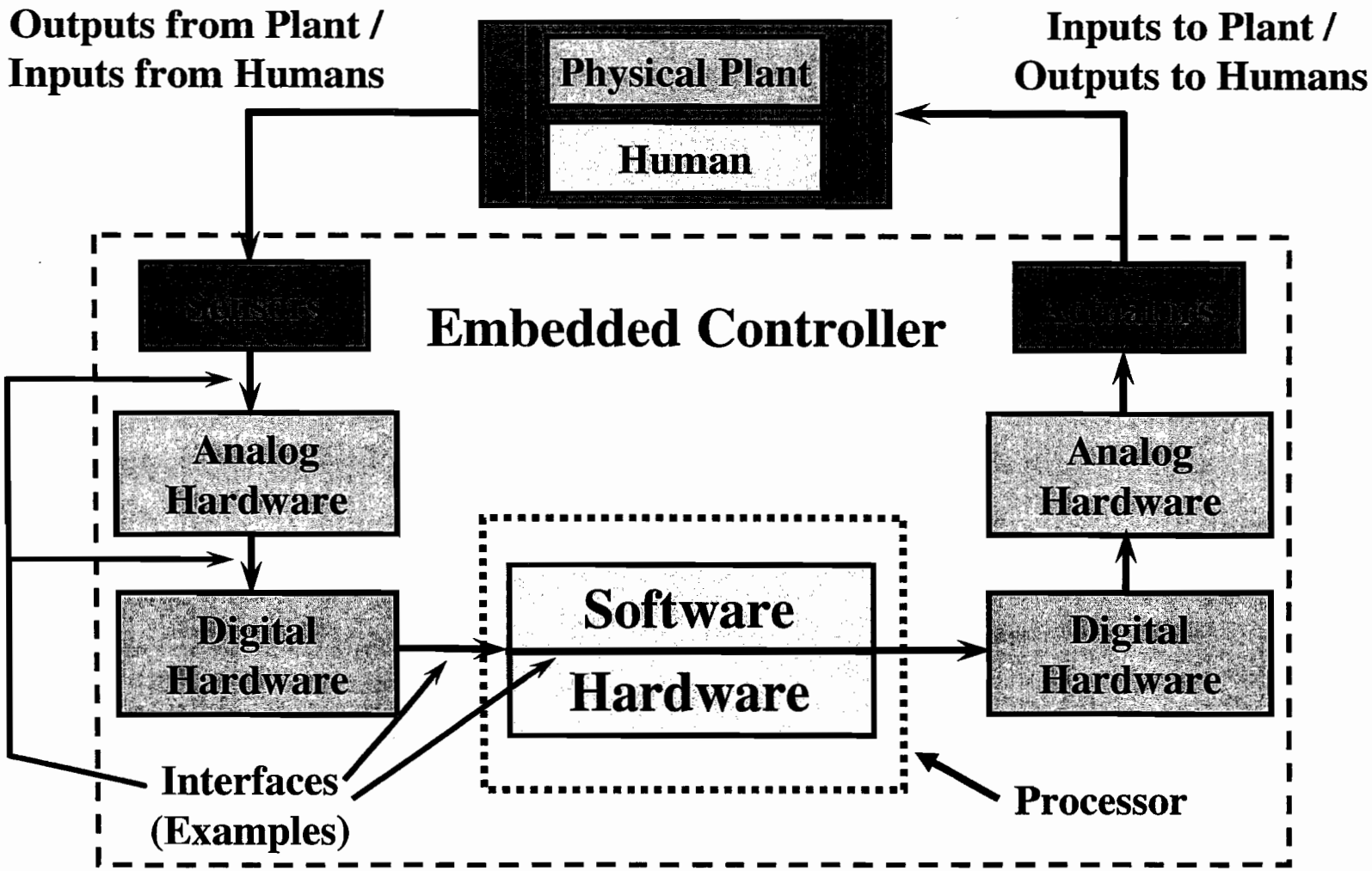
- A safety assessment process has been developed based on fault injection techniques and the consideration of the integrated hardware/software system
- The process has been applied to multiple practical commercial applications and approved by an independent safety assessors (e.g. TUV Rheinland)
- We are currently developing new fault models and new statistical models to support the approach
- We are currently developing new modeling and fault injection techniques based on COTS software tools (Simics)
- Digital feedwater control systems application successfully completed

Research Objectives

- Develop a safety assessment methodology for digital systems
  - Consider the integrated hardware/software system
  - Include commercial-off-the-shelf (COTS) hardware and software
- Develop modeling, simulation, and experimental techniques that support the assessment methodology
  - Support the estimation of quantitative metrics
  - Support the evaluation of qualitative attributes
- Develop tools that support the safety assessment methodology
  - Use COTS software tools where feasible
  - Create new tools where needed
- Demonstrate the resulting approach and tools on real examples
  - Nuclear reactor systems
  - Railway systems
  - Aircraft flight control systems
  - Other examples

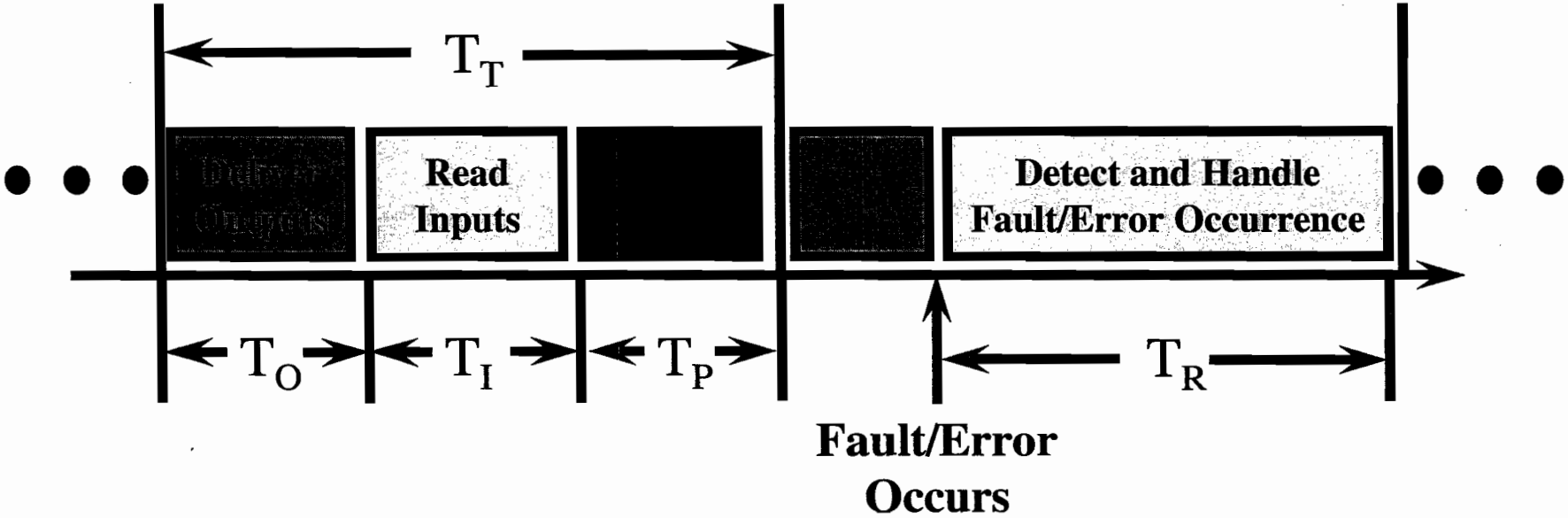
Background

Structure of Digital Systems



Background

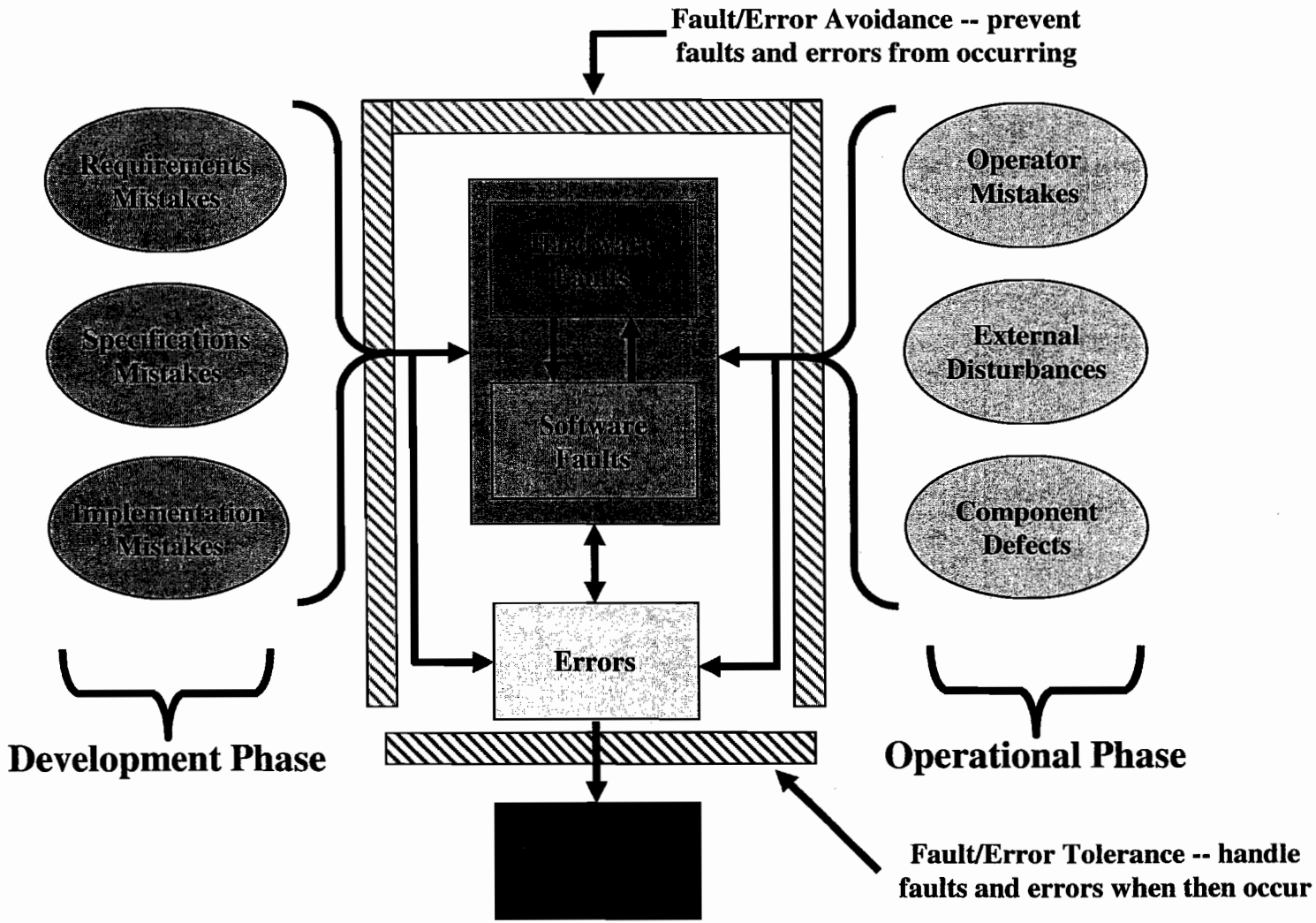
Real-Time Requirements



T_O -- maximum output delivery time
T_I -- maximum input collection time
T_P -- maximum processing time
T_T -- maximum sampling period
T_R -- maximum time to handle faults

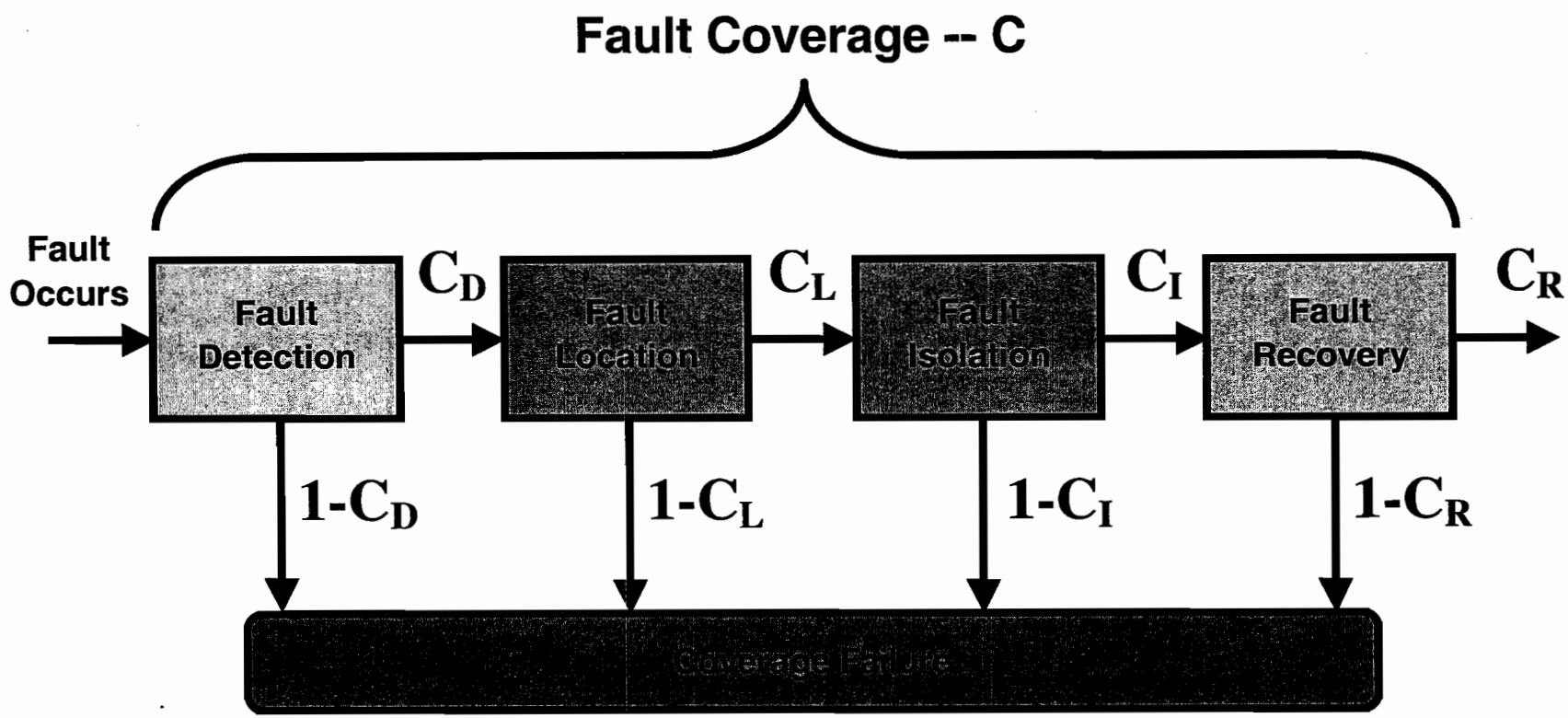
Background

Causes and Effects of Faults



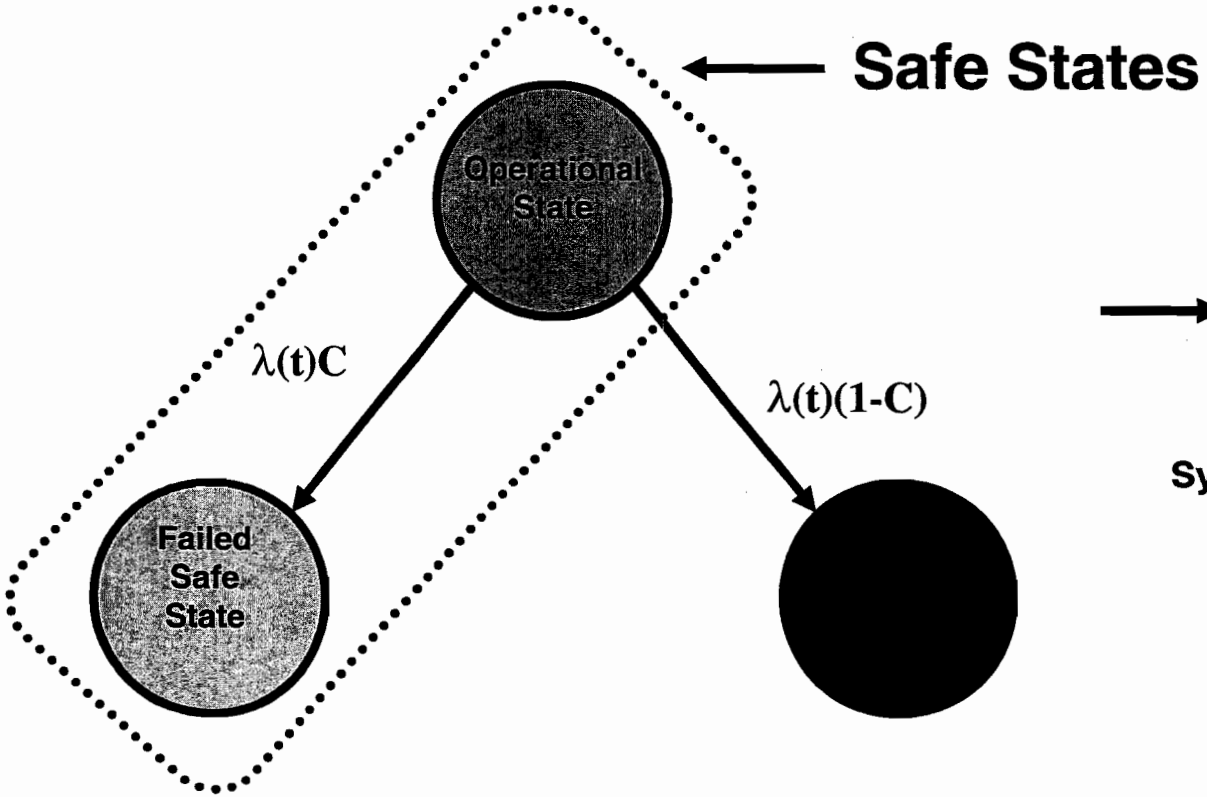
Background

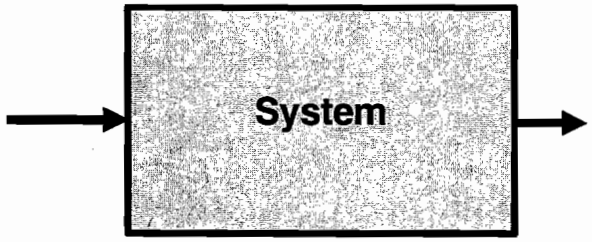
Concept of Fault Coverage



Background

Simple Three-State System Safety Model





System Failure Rate = $\lambda(t)$
Coverage = C

- **Fault Coverage (C) – the conditional probability that a system correctly handles a fault, given that a fault has occurred**

Background

Safety, S(t)

- Safety, S(t) – the probability that a system will either perform its functions correctly or will discontinue its functions in a defined safe manner.

- For the simple three-state safety model S(t) can be expressed as the probability of being in either the "operational" or "failed-safe" states.

- Steady-State Safety (S_{ss}) can be expressed as

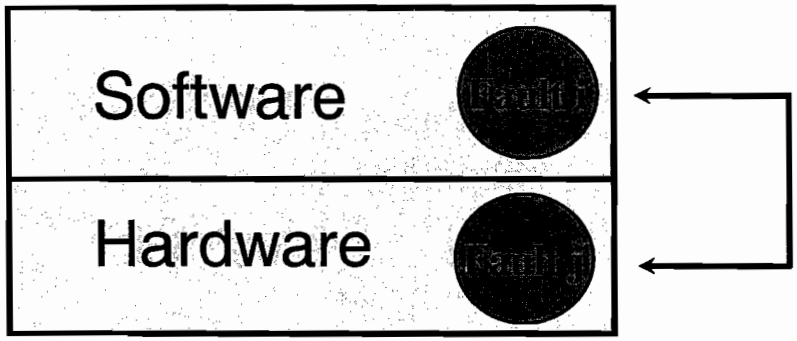
$$S_{ss} = \lim_{t \to \infty} S(t)$$

- The fault coverage represents a conservative estimate of the lower bound on Steady-State Safety

- For the simple three-state safety model, $S_{ss} = C$

Challenges

Hardware and Software are not Independent

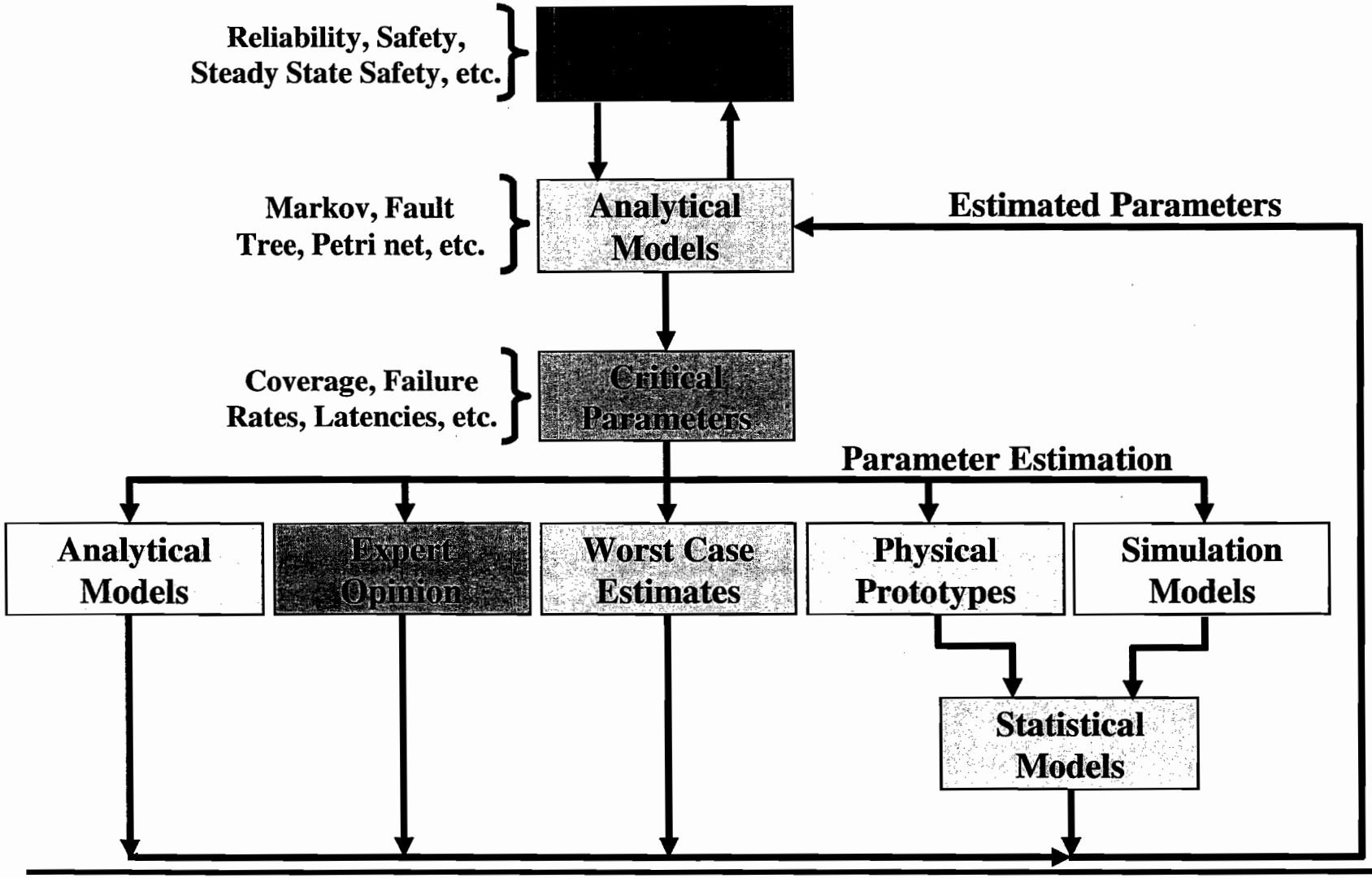


What happens when faults occur in both the hardware and software?

- **Software must execute on a hardware platform. The operation of the integrated hardware/software system is critical.**
- **A fault in software (Fault i) in combination with a fault in hardware (Fault j) can result in unsafe conditions and/or unreliable operation.**
- **Much of the software in safety-critical systems is designed to handle fault detection, fault location, fault isolation, and fault recovery. Such software is often unexercised.**

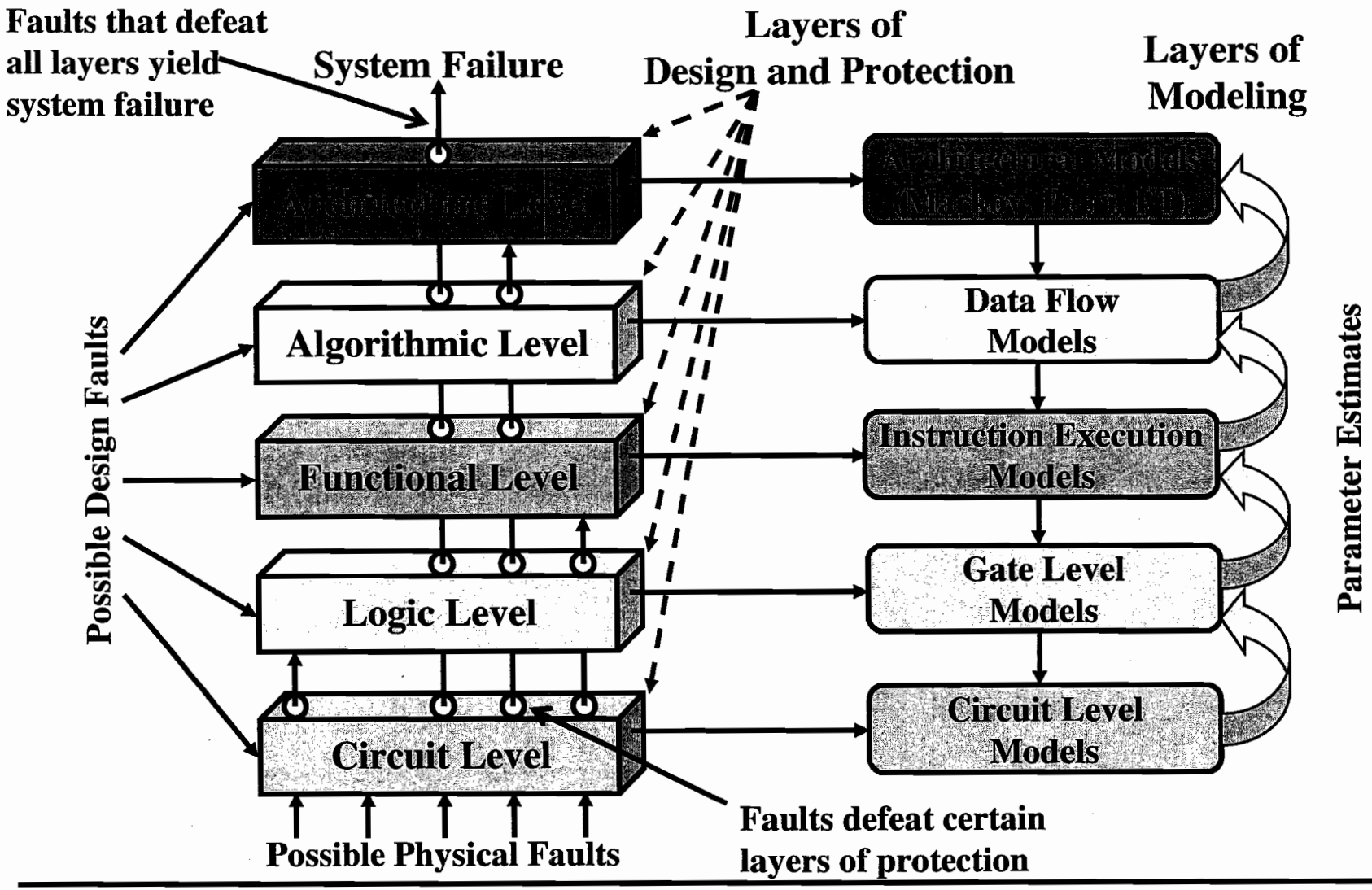
System Modeling Methodology

Overview of the Process



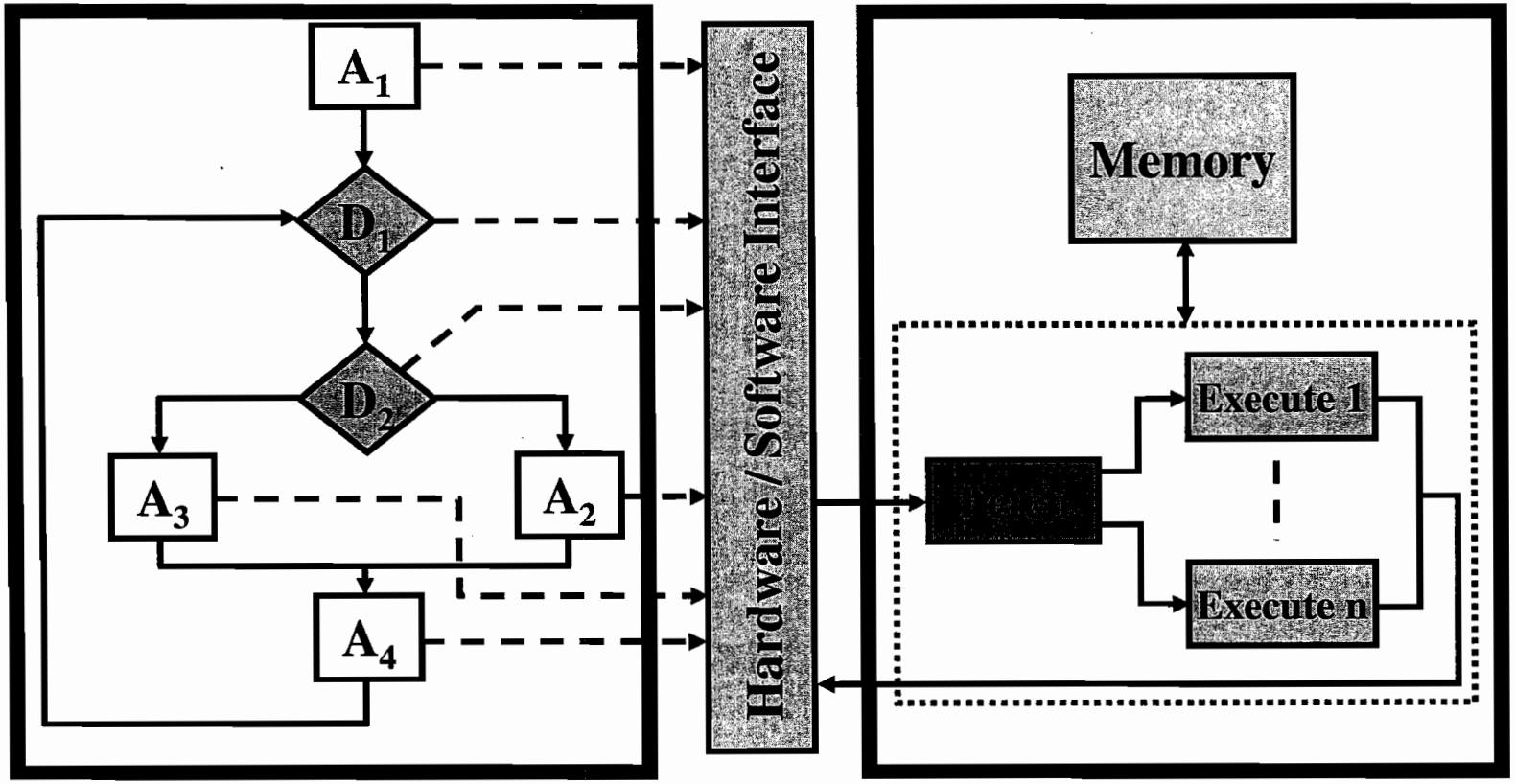
System Modeling Methodology

Hierarchical Approach



System Modeling Metholodology

Hardware/Software Integrated Modeling



Software Model

-- Data Flow

-- Actual Code

Hardware Model

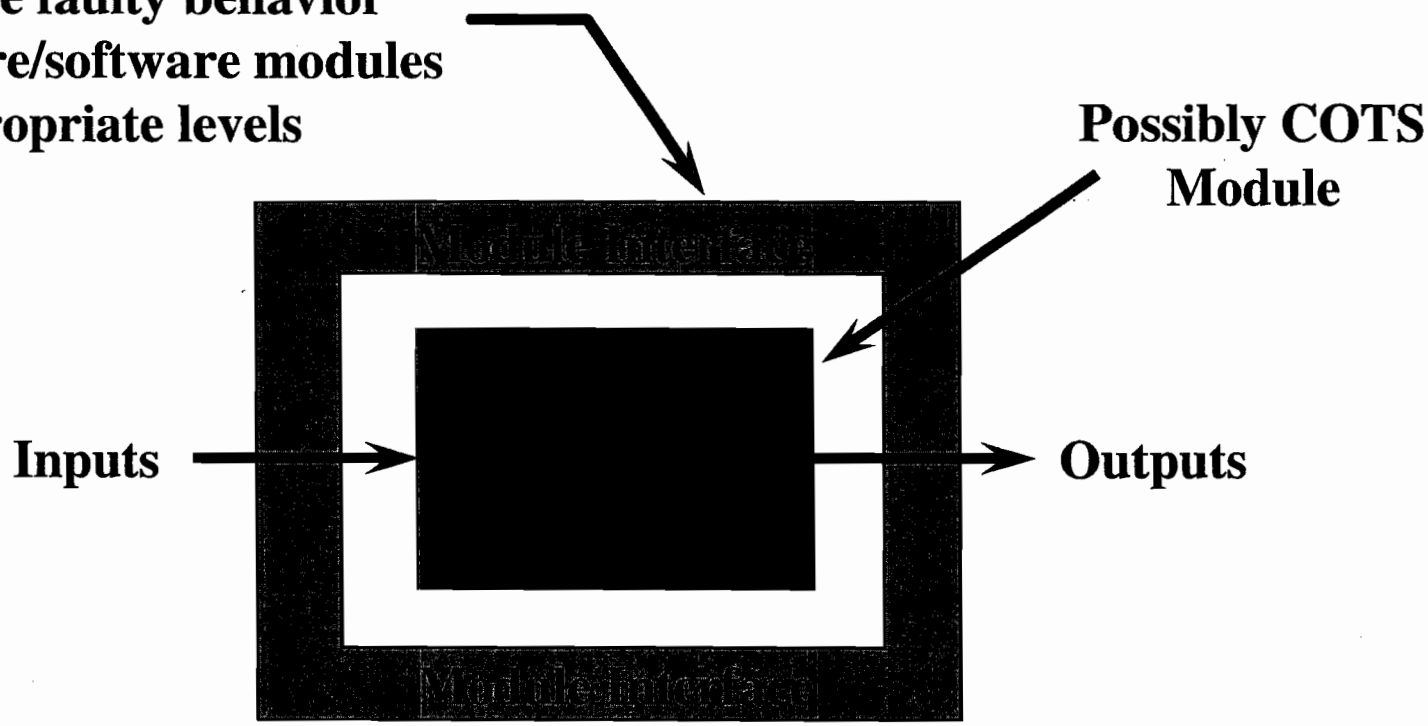
-- Execution Model

-- Gate-level Model

System Modeling Methodology

Characterization of Faulty Behavior

Models are developed which describe the faulty behavior of hardware/software modules at the appropriate levels



Examples of UVA Research

Johnson, B. and Aylor, J., "Reliability and Safety Anaylsis of a Fault-Tolerant Controller", *IEEE Transactions on Reliability*, Vol. 35, No. 4, Oct. 1986, pp. 355-362.

Welke, S., Johnson, B., and Aylor, J. "Reliability Modeling of Hardware/Software Systems", *IEEE Transactions on Reliability*, Vol. 44, No. 3, Sept. 1995, pp. 413-418.

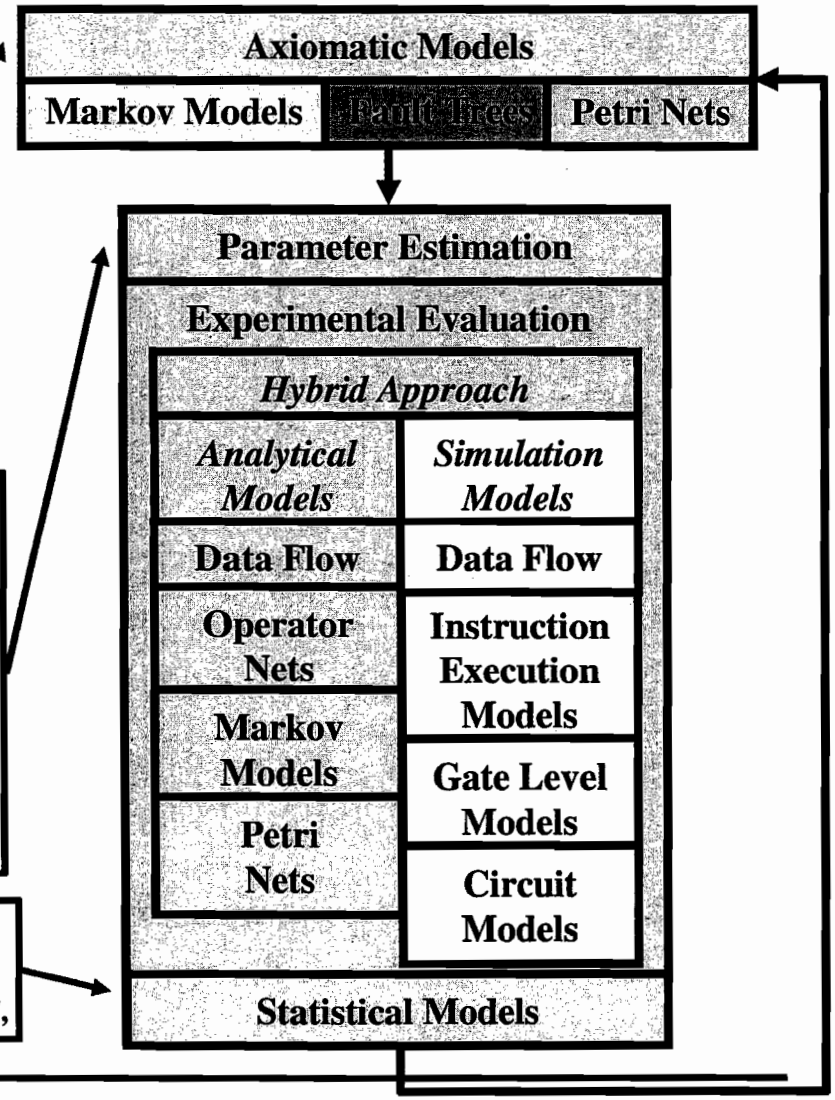
Choi, C., Johnson, B., and Profeta, III, J., "Safety Issues in the Comparative Analysis of Dependable Architectures", *IEEE Transactions on Reliability*, Vol. 46, No. 3, Sept. 1997, pp. 316-322.

Smith, D., Johnson, B., and Profeta, III, J., "System Dependability Evaluation Using a Fault List Generation Algorithm", *IEEE Transactions on Computers*, Vol. 45, No. 8, Aug. 1996, pp. 974-979.

Kaufman, L. M., Johnson, B. W., and Bechta Dugan, J., "Coverage Estimation Using Statistics of Extremes for When Testing Reveals No Failures", *IEEE Transactions on Computers*, Vol. 51, No. 1, January 2002, pp. 3-12.

DeLong, T, Johnson, B., and Profeta, III, J., "A Fault Injection Technique for VHDL Behavioral-Level Models", *IEEE Design and Test of Computers*, Vol. 13, No. 4, Mar. 1996, pp. 24-33.

Smith, D., Johnson, B., Andrianos, N, and Profeta, III, J., "A Variance Reduction Technique Using Fault Expansion for Fault Coverage Estimation", *IEEE Transactions on Reliability*, Vol. 46, No. 3, Sept. 1997, pp. 366-374.



Examples of UVA Research (Continued)

- Theoretical foundation of safety assessment process
  - Ideas were created while in industry (Harris Corporation)
  - Ideas applied to Harris helicopter flight control system
- Modeling and Simulation Tools
  - ADEPT was the first implementation of system modeling techniques (funded by DARPA, NSF, and NASA)
  - ROBUST was first hierarchical fault simulation tool (funded by U.S. Air Force)
- Peer Review of Research
  - Research began in 1984 and has been continuously funded by NASA, NSF, DARPA, IBM, Hughes, SRC, Boeing, Ansaldo, FRA, Lockheed Martin, and others
  - 10 PhDs and 32 MS students have received degrees working on the research topics (4 PhDs in progress)
  - More than 125 peer-reviewed publications and 1 patent
  - Named IEEE Fellow for contributions

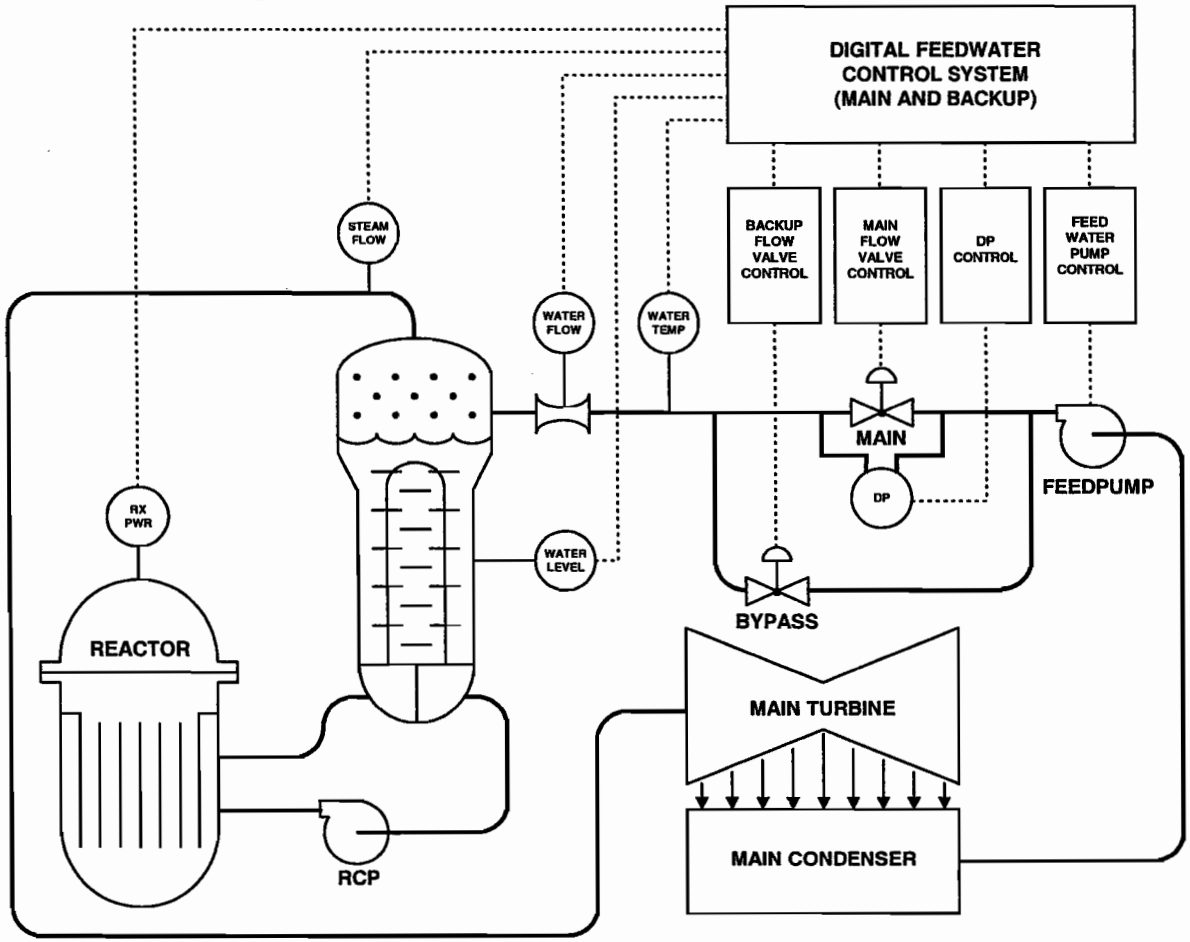
Applications

- Los Angeles Metro Green Line Transit System
  - Actual software executing on a hardware model
  - Results obtained for more than 10 billion experiments
  - Uncovered three software design faults
  - Results approved by California Public Utility Commission
- Copenhagen Metro System
  - Physical prototype running complete software system
  - Gate-level simulations of a complete 32-bit processor
  - Uncovered one software design fault
  - Approved by TUV Rheinland (Cologne, Germany)
- Other systems currently being analyzed
  - Calvert Cliffs Digital Feedwater Control System
  - New York City Transit Authority train control system
  - CSX communication-based train control system (Georgia)
  - Magnetically levitated train system (Pittsburgh)
  - Illinois Department of Transportation train control system

Applications

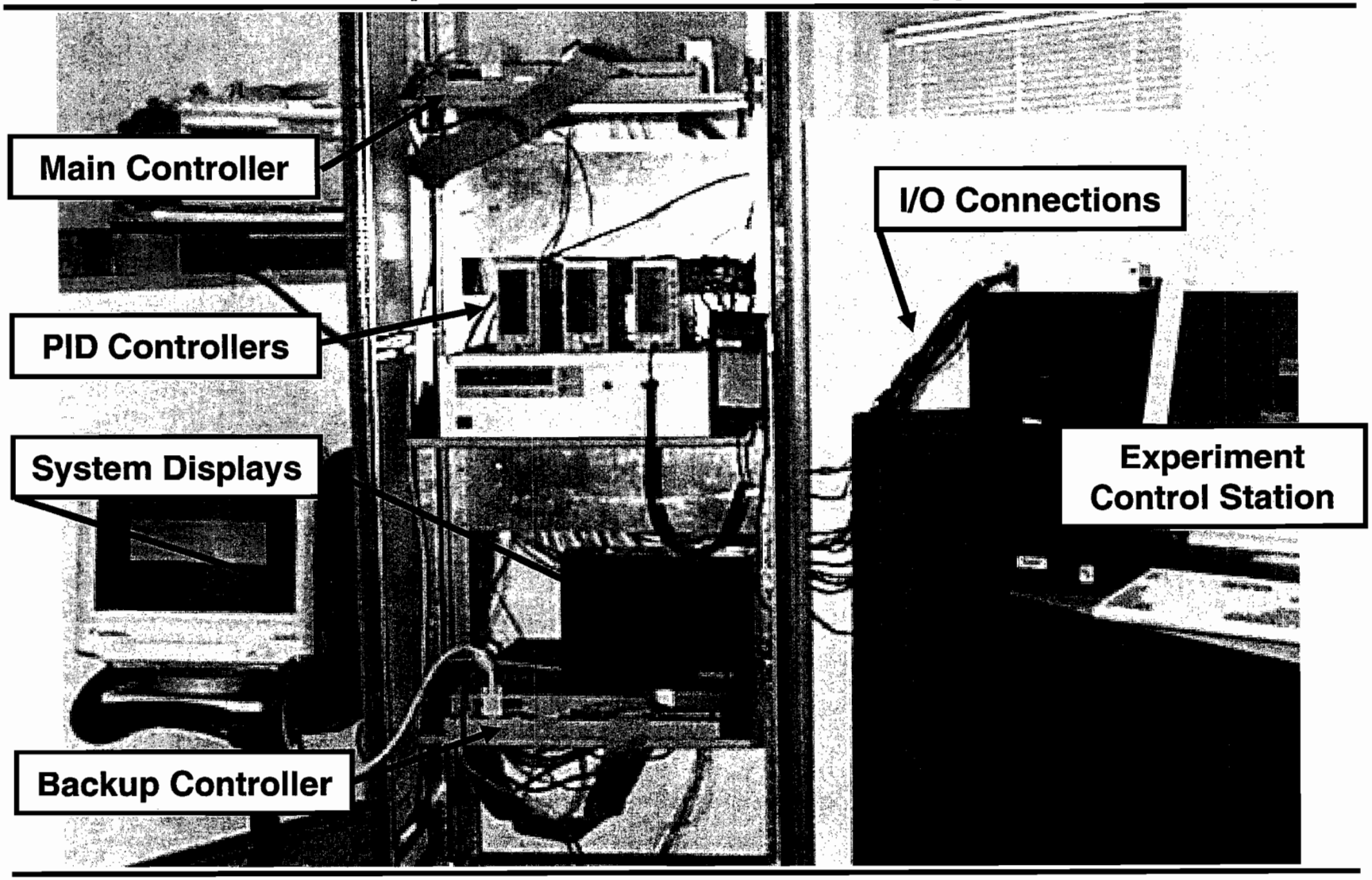
Overview of Calvert Cliffs DFWCS

- **Purpose: control the water level in its associated steam generator from ~1% to 100% power**



Applications

Experimental DFWCS Prototype

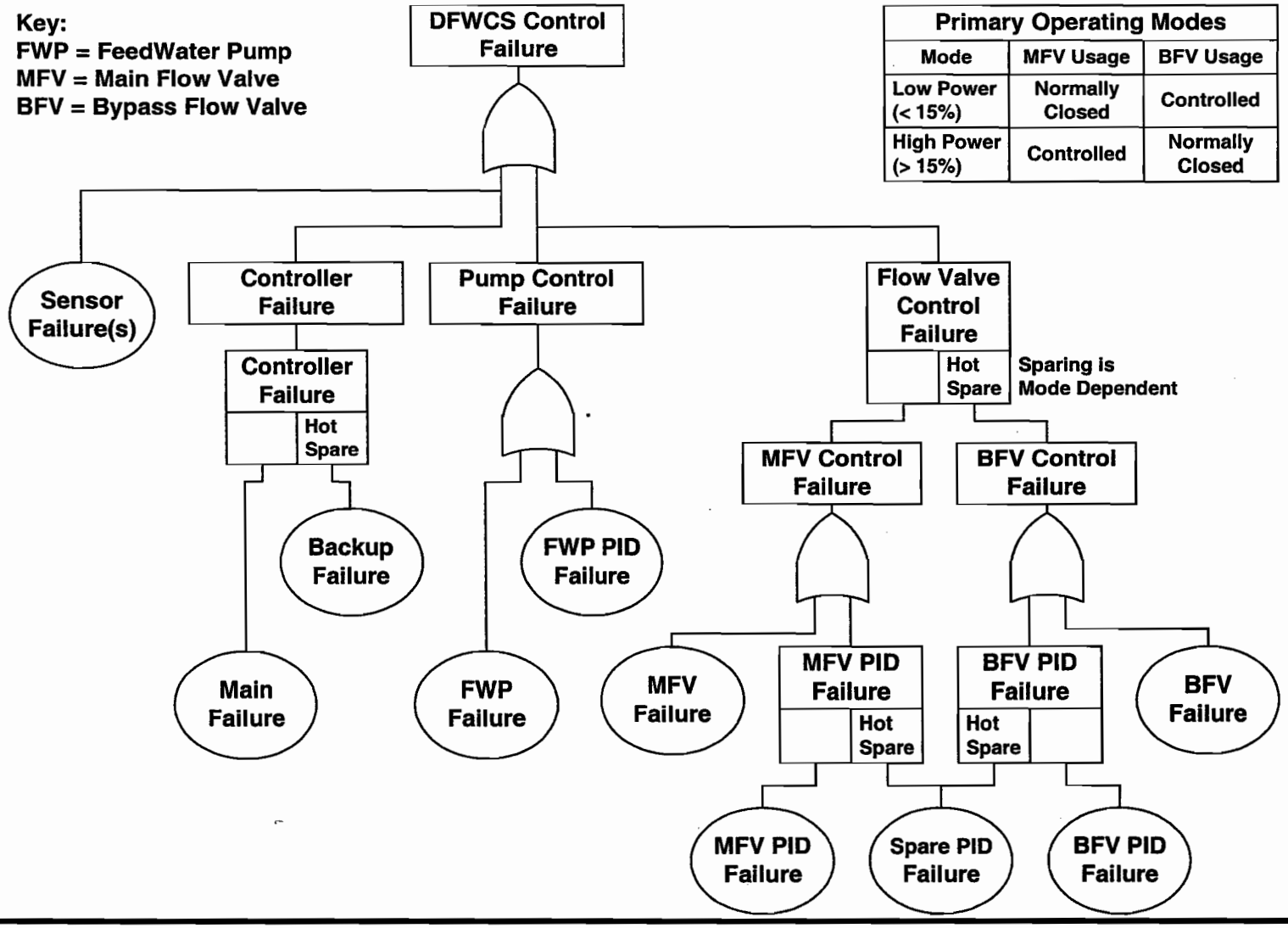


Applications

Dynamic Fault Tree Model for DFWCS

Key:
FWP = FeedWater Pump
MFV = Main Flow Valve
BFV = Bypass Flow Valve

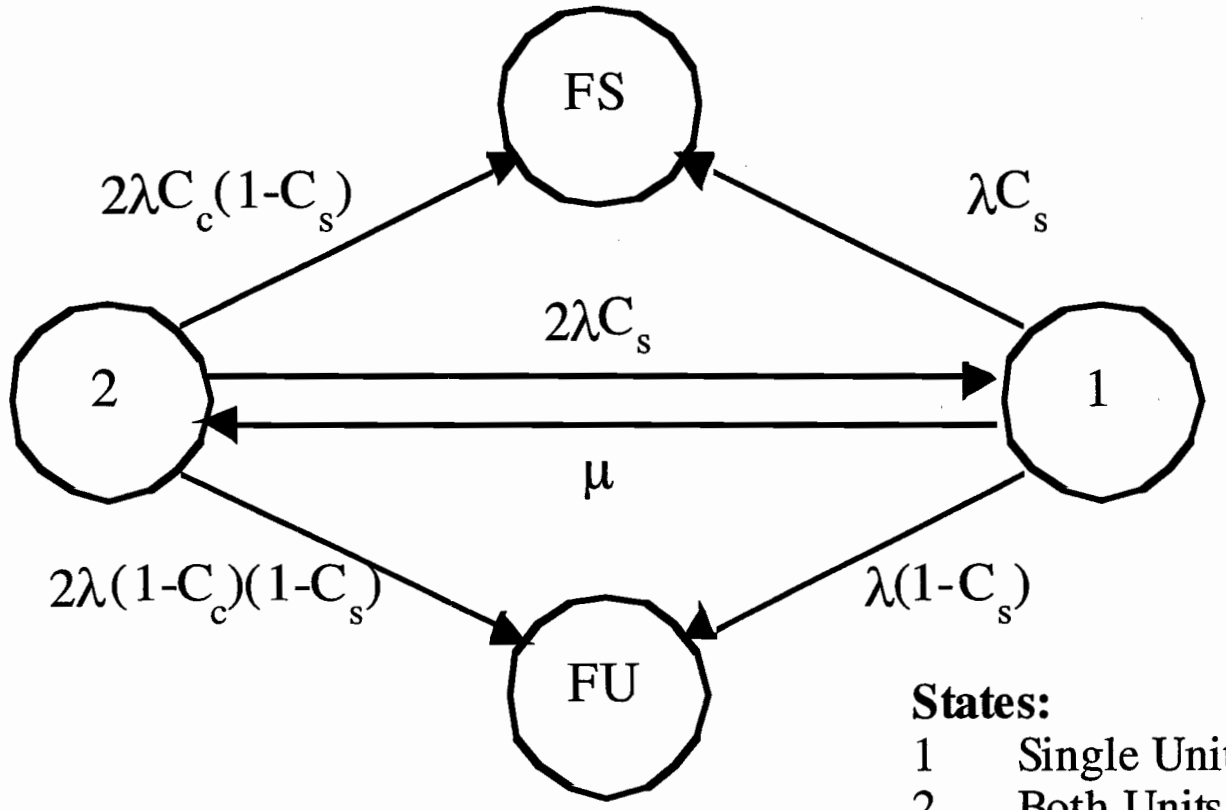
Primary Operating Modes		
Mode	MFV Usage	BFV Usage
Low Power (< 15%)	Normally Closed	Controlled
High Power (> 15%)	Controlled	Normally Closed



Applications

Conversion to a Markov Model

- **The resulting Markov model**



States:

1	Single Unit Operational
2	Both Units Operational
FS	Failed-Safe
FU	Failed-Unsafe

Applications

MTTUF and S_{ss} Expressions

- **Resulting MTTUF Expression:**

$$MTTUF = \frac{1 + 2C_s}{2\lambda(1 - C_s)[1 - C_c + C_s]}$$

- **Resulting S_{ss} Expression:**

$$S_{ss} = C_c(1 - C_s) + C_s^2$$

Reference

Choi, C., Johnson, B., and Profeta, III, J., "Safety Issues in the Comparative Analysis of Dependable Architectures", *IEEE Transactions on Reliability*, Vol. 46, No. 3, Sept. 1997, pp. 316-322.

Applications

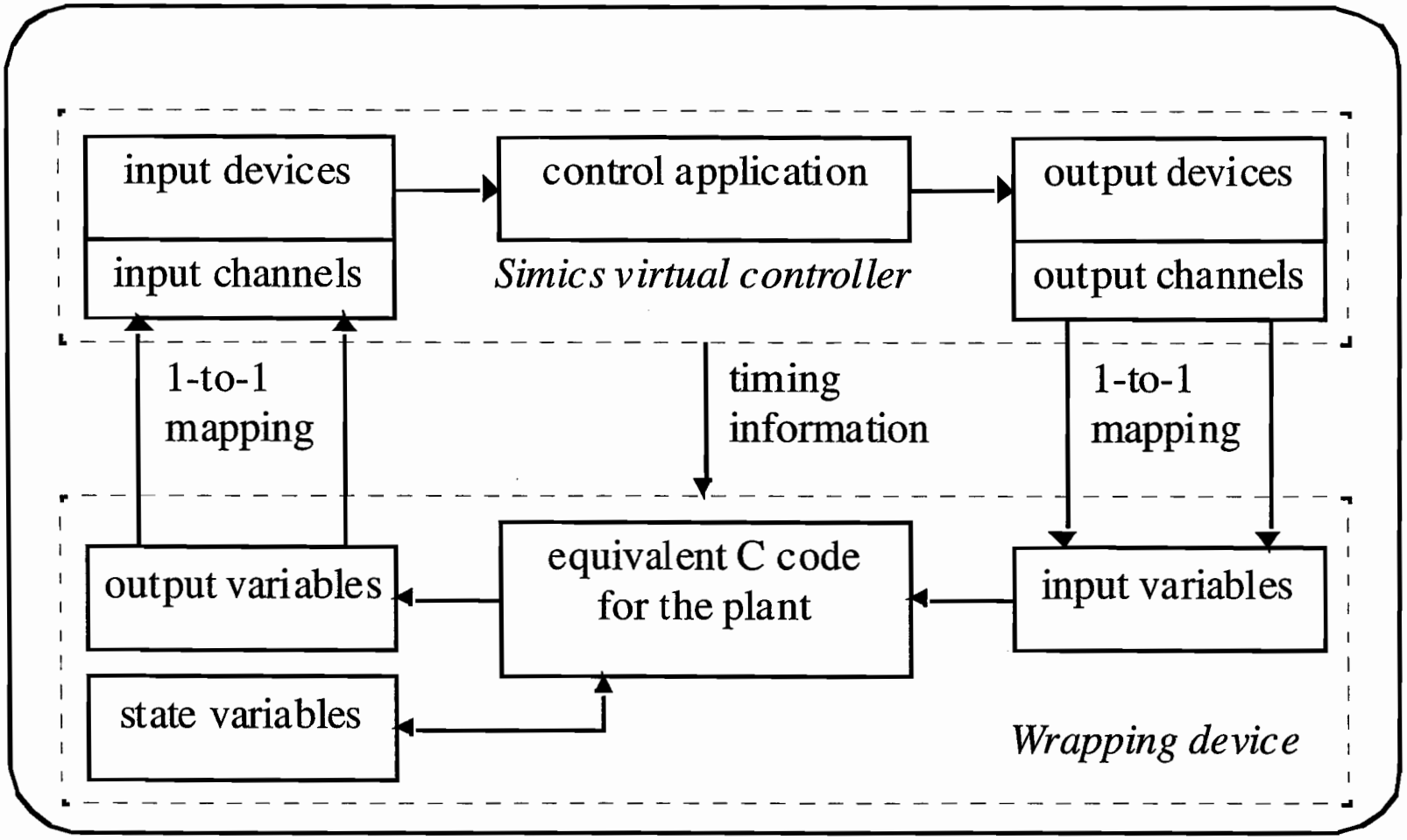
Fault Injection Techniques for DFWCS

- Two approaches were investigated: Software-based and Simulation-based fault injection
  - Both fault injection approaches center around assessment of the Main Controller
- Software-based fault injection approach
  - Uses software interrupts in operating system to modify register and memory contents during execution of the DFWCS software
- Simulation-based fault injection approach
  - Uses COTS simulation tool (Simics) to seamlessly replace the Main Controller hardware with a simulation model
  - Tool allows access to complete programmer's model of the system to perform fault injection

Applications

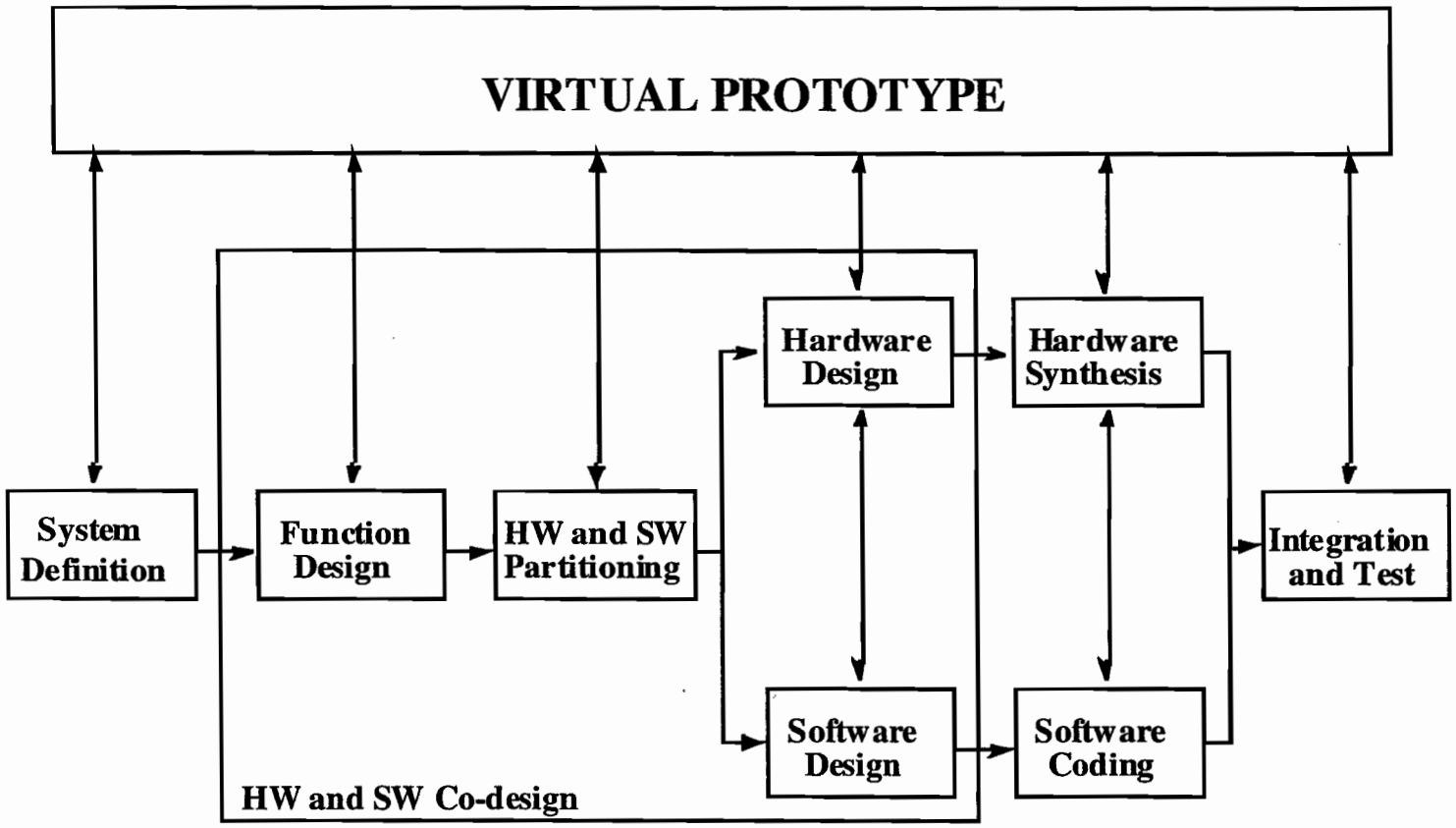
Simulation Environment and Capabilities

Simics simulation framework



Future Research Goal

Design and Assessment Process



Summary

- A safety assessment process has been developed based on fault injection techniques and the consideration of the integrated hardware/software system
- The process has been applied to multiple practical commercial applications and approved by an independent safety assessors (e.g., TUV Rheinland)
- Toolsets and computing resources are being developed to allow safety/reliability assessment over the web
  - Equipment under evaluation stays at supplier's facility
- We are currently developing new fault models and new statistical models to support the approach
- We are currently developing new modeling and fault injection techniques based on COTS software tools (Simics)